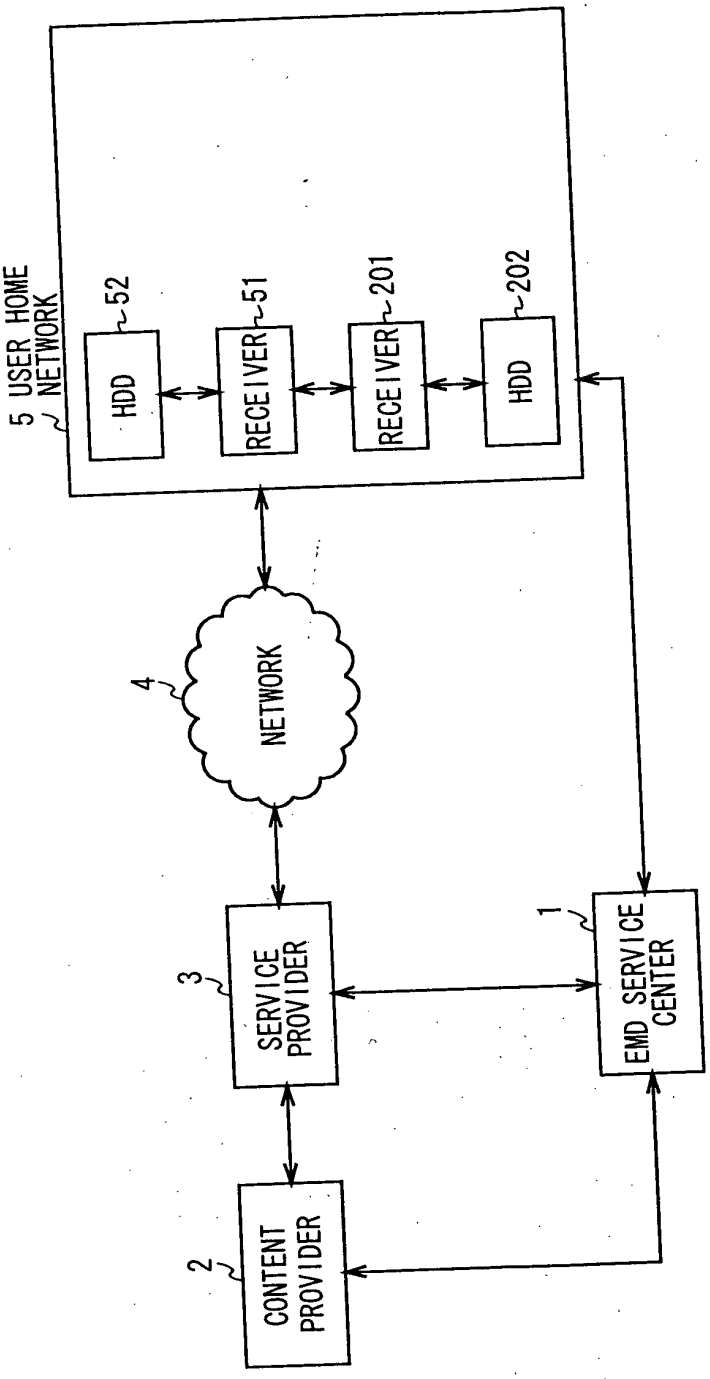

5 USER HOME NETWORK
HDD
52
RECEIVER
51
RECEIVER
201
HDD
202
NETWORK
4
SERVICE PROVIDER
3
EMD SERVICE CENTER
1
CONTENT PROVIDER
2

FIG. 1

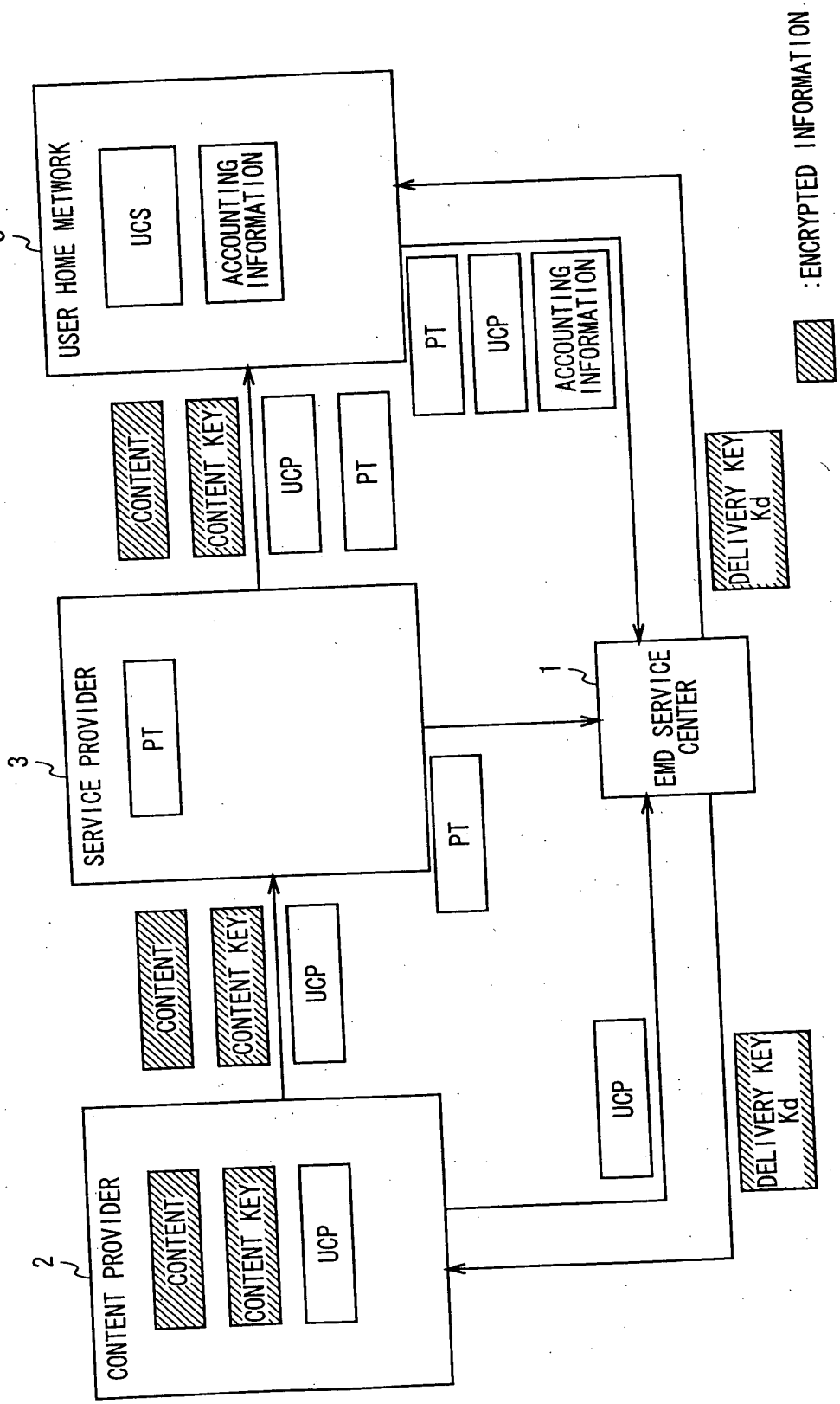
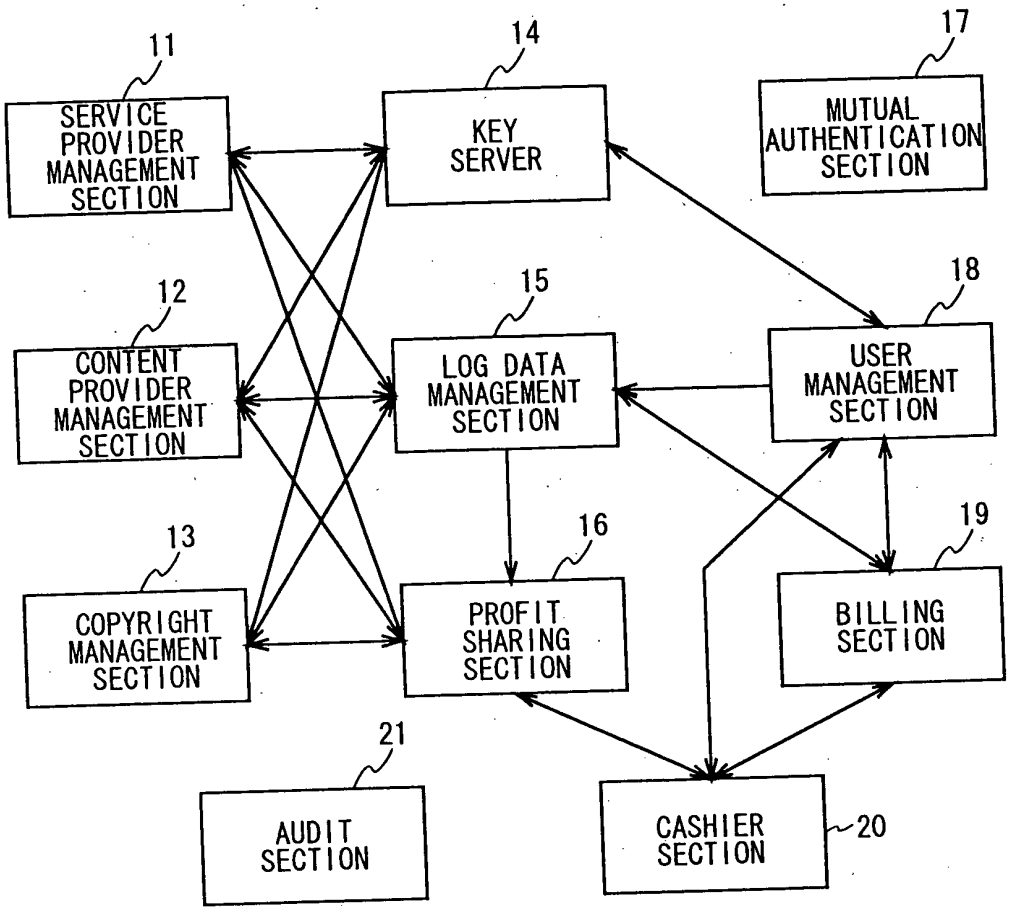

USER HOME METWORK
5
UCS
ACCOUNTING INFORMATION
CONTENT
CONTENT KEY
UCP
PT
PT
UCP
ACCOUNTING INFORMATION
DELIVERY KEY Kd
:ENCRYPTED INFORMATION
SERVICE PROVIDER
3
PT
PT
1
EMD SERVICE CENTER
CONTENT
CONTENT KEY
UCP
UCP
DELIVERY KEY Kd
CONTENT PROVIDER
2
CONTENT
CONTENT KEY
UCP

FIG. 2



EMD SEVICE CENTER 1

FIG. 3

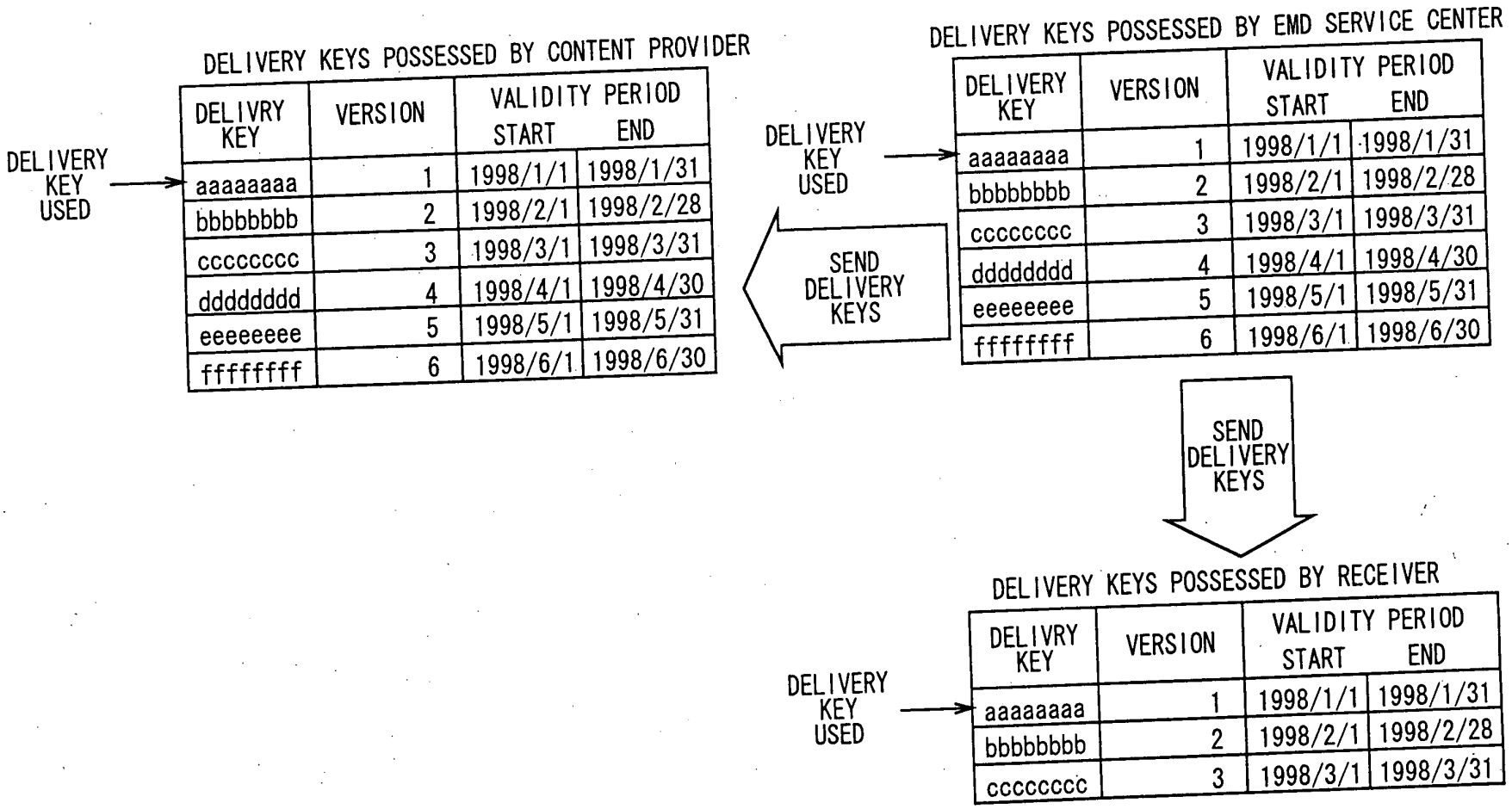


FIG. 4

09/719015

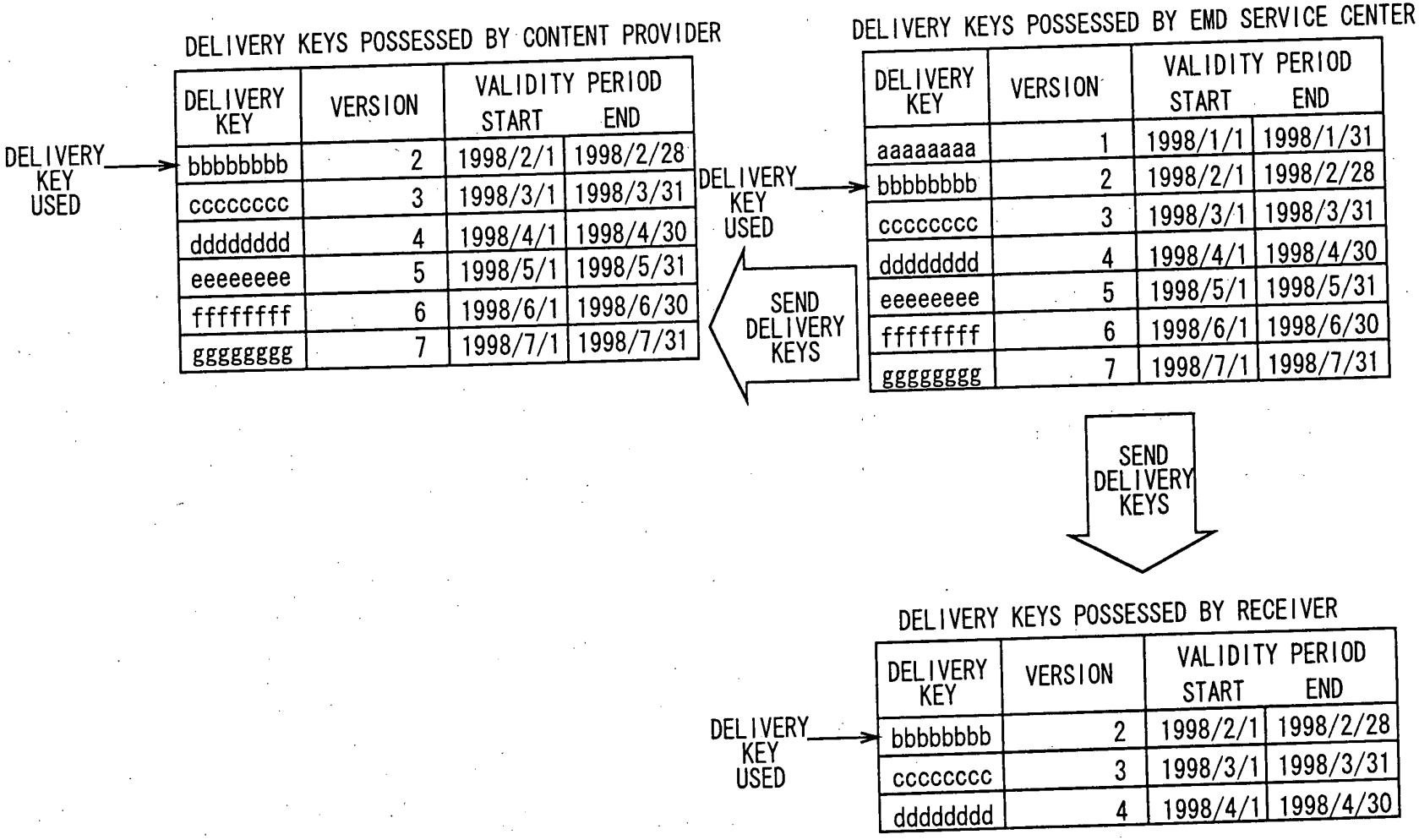
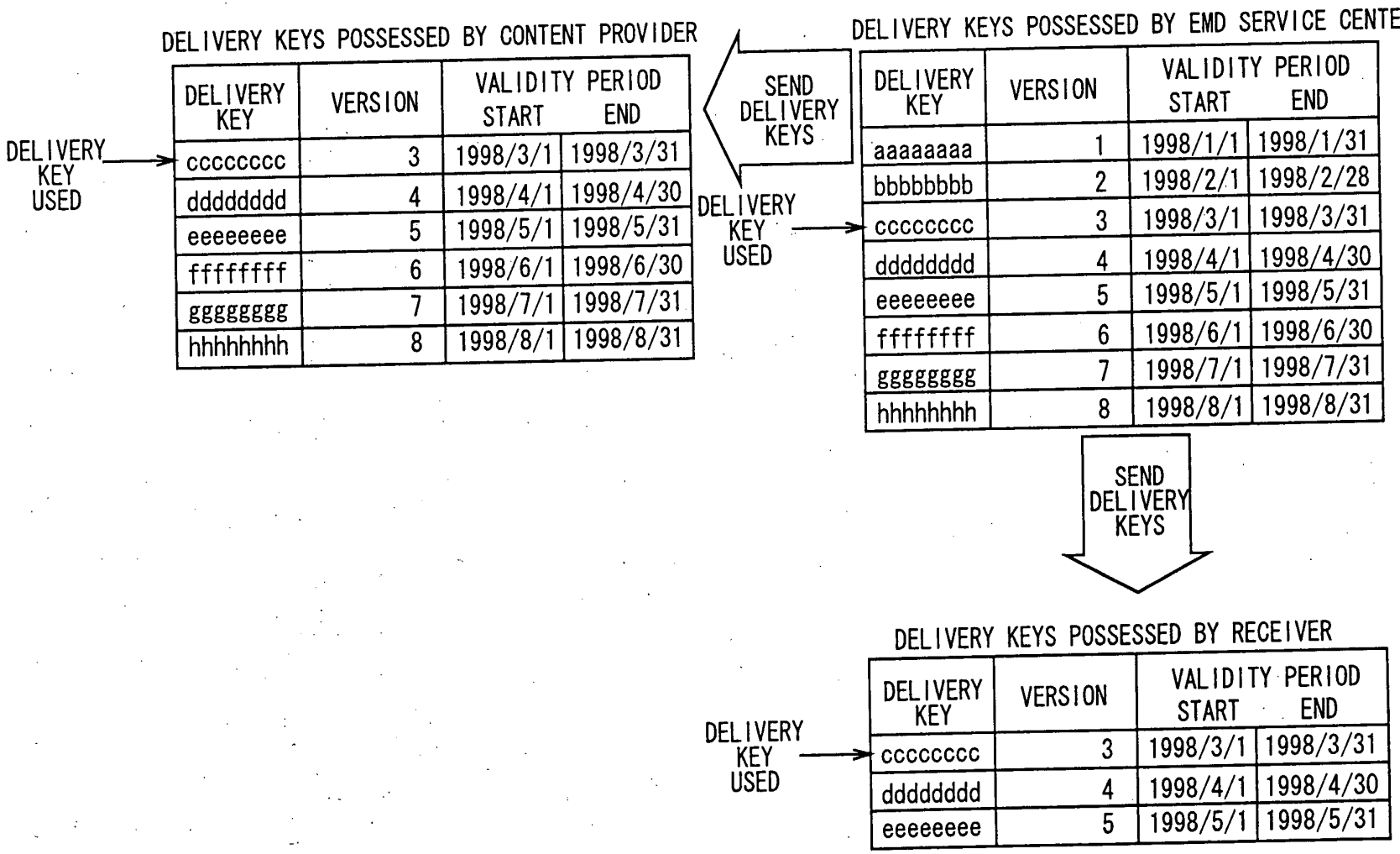


FIG. 5

09/719015

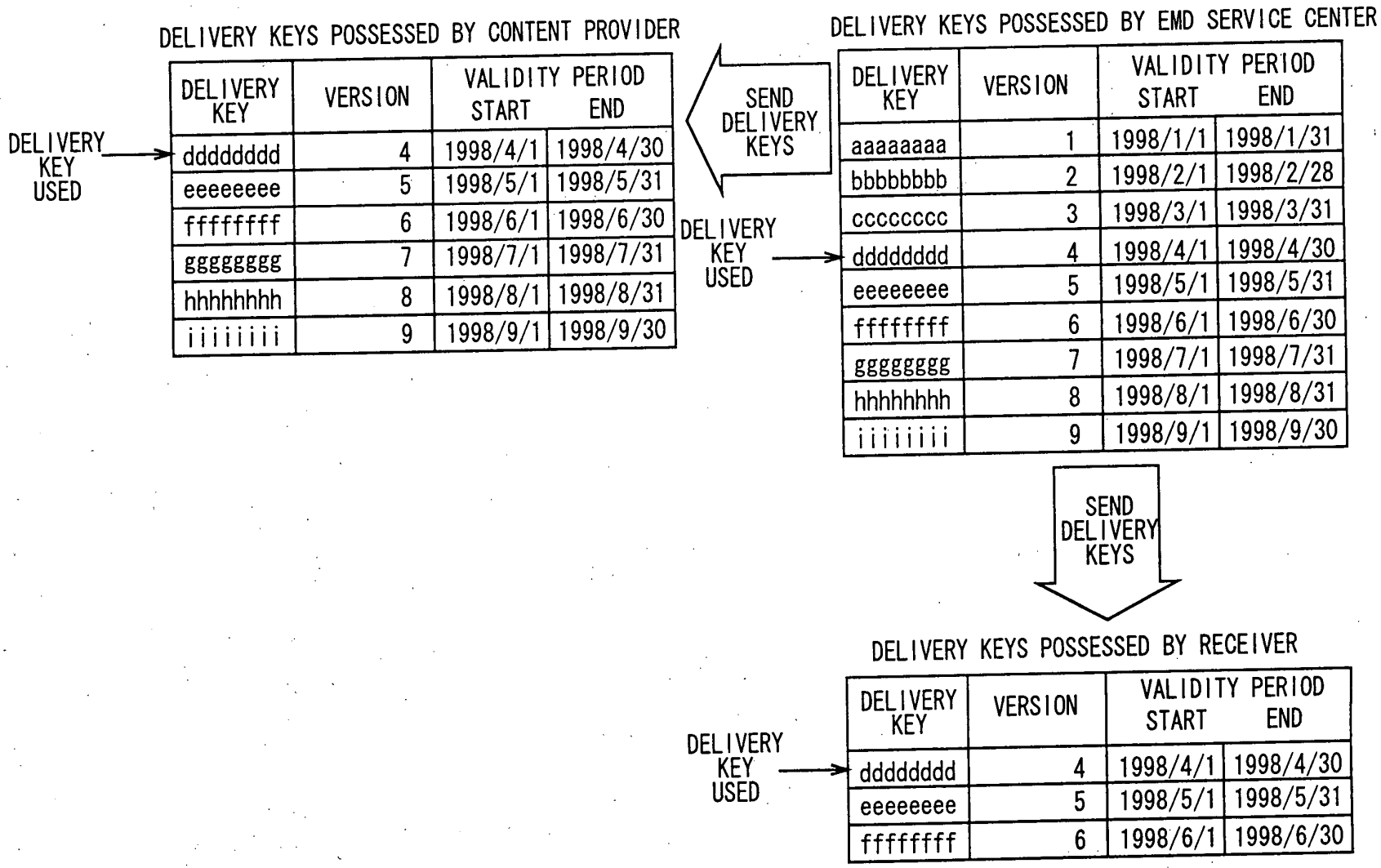


DELIVERY KEY	VERSION	VALIDITY PERIOD START	VALIDITY PERIOD END
cccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30
gggggggg	7	1998/7/1	1998/7/31
hhhhhhhh	8	1998/8/1	1998/8/31

DELIVERY KEY	VERSION	VALIDITY PERIOD START	VALIDITY PERIOD END
aaaaaaaa	1	1998/1/1	1998/1/31
bbbbbbbb	2	1998/2/1	1998/2/28
cccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30
gggggggg	7	1998/7/1	1998/7/31
hhhhhhhh	8	1998/8/1	1998/8/31

DELIVERY KEY	VERSION	VALIDITY PERIOD START	VALIDITY PERIOD END
cccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31

FIG. 6

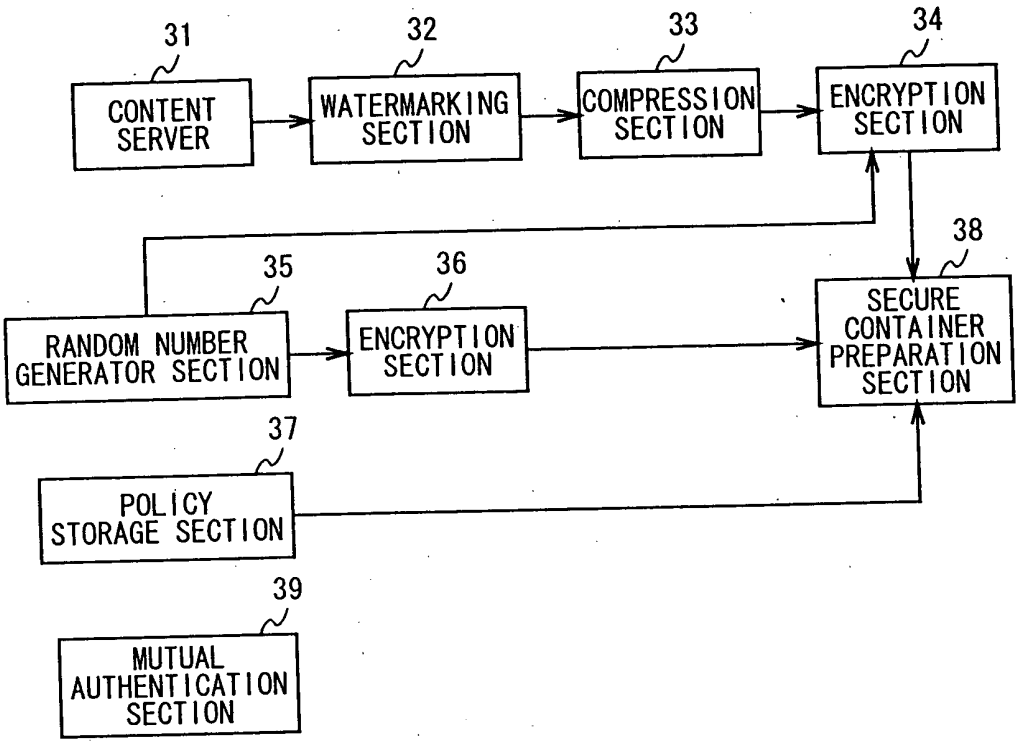


DELIVERY KEY	VERSION	VALIDITY PERIOD START	END
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30
gggggggg	7	1998/7/1	1998/7/31
hhhhhhhh	8	1998/8/1	1998/8/31
iiiiiiii	9	1998/9/1	1998/9/30

DELIVERY KEY	VERSION	VALIDITY PERIOD START	END
aaaaaaaa	1	1998/1/1	1998/1/31
bbbbbbbb	2	1998/2/1	1998/2/28
cccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30
gggggggg	7	1998/7/1	1998/7/31
hhhhhhhh	8	1998/8/1	1998/8/31
iiiiiiii	9	1998/9/1	1998/9/30

DELIVERY KEY	VERSION	VALIDITY PERIOD START	END
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30

FIG. 7



CONTENT PROVIDER 2

FIG. 8

CONTENT ID	ID OF CONTENT A	
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2	
UCP ID	ID OF UCPA	
UCP VALIDITY	VALIDITY PERIOD OF UCPA	
USAGE CONDITIONS 10	USER CONDITIONS 10	200 POINTS OR HIGHER
	EQUIPMENT CONDITIONS 10	NO CONDITION
USAGE DETAILS 11	ID 11	ID OF USAGE DETAILS 11
	TYPE 11	PURCHASE AND REPRODUCE
	PARAMETER 11	× × × ×
	CONTROL TRANSFER PERMISSION INFORMATION 11	PERMITTED
USAGE DETAILS 12	ID 12	ID OF USAGE DETAILS 12
	TYPE 12	FIRST-GENERATION DUPLICATE
	PARAMETER 12	× × × ×
	CONTROL TRANSFER PERMISSION INFORMATION 12	NOT PERMITTED
USAGE DETAILS 13	ID 13	ID OF USAGE DETAILS 13
	TYPE 13	LIMITED-TIME REPRODUCTION
	PARAMETER 13	× × × ×
	CONTROL TRANSFER PERMISSION INFORMATION 13	NOT PERMITTED
USAGE DETAILS 14	ID 14	ID OF USAGE DETAILS 14
	TYPE 14	Pay Per Copy 5
	PARAMETER 14	DUPLICATES FIVE TIMES
	CONTROL TRANSFER PERMISSION INFORMATION 14	NOT PERMITTED

A

UCPA

B

CONTENT ID		ID OF CONTENT A
CONTENT PROVIDER ID		ID OF CONTENT PROVIDER 2
UCP ID		ID OF UCPB
UCP VALIDITY PERIOD		VALIDITY PERIOD OF UCPB
USAGE DETAILS 20	USER CONDITIONS 20	200 POINTS OR LOWER
	EQUIPMENT CONDITIONS 20	NO CONDITION
USAGE DETAILS 21	ID 21	ID OF USAGE DETAILS 21
	TYPE 21	Pay Per Play 4
	PARAMETER 21	REPRODUCTION FOUR TIMES
	CONTROL TRANSFER PERMISSION INFORMATION 21	NOT PERMITTED
USAGE DETAILS 22	ID 22	ID OF USAGE DETAILS 22
	PARAMETER 22	Pay Per Copy 2
	PARAMETER 22	DUPLICATES TWO TIMES
	CONTROL TRANSFER PERMISSION INFORMATION 22	NOT PERMITTED

UCPB

FIG. 9

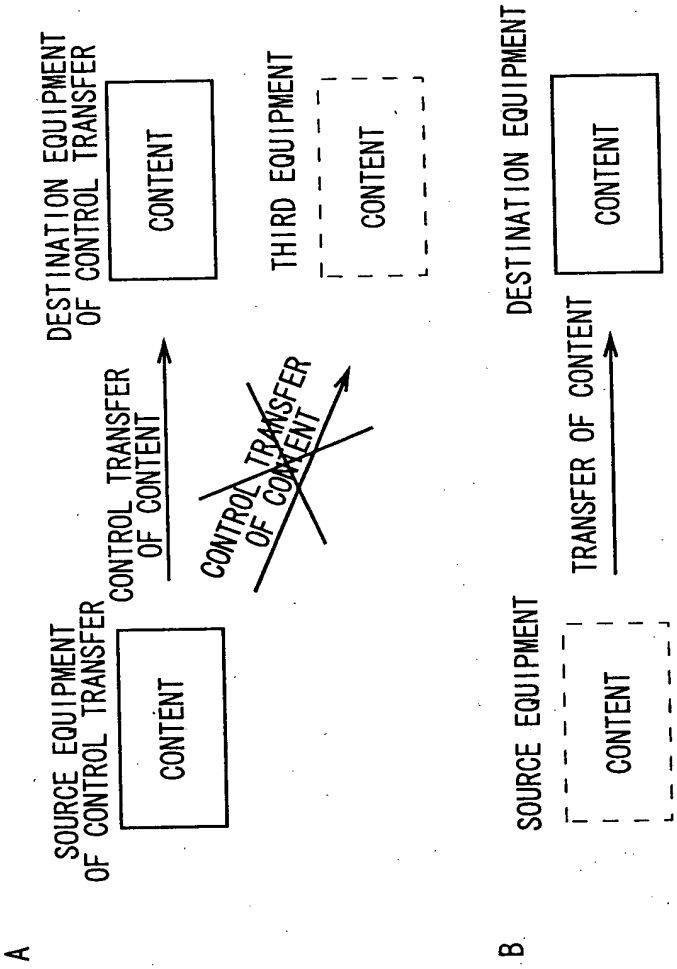

A
SOURCE EQUIPMENT OF CONTROL TRANSFER
CONTENT
CONTROL TRANSFER OF CONTENT
CONTROL TRANSFER OF CONTENT
DESTINATION EQUIPMENT OF CONTROL TRANSFER
CONTENT
THIRD EQUIPMENT
CONTENT
B
SOURCE EQUIPMENT
CONTENT
TRANSFER OF CONTENT
DESTINATION EQUIPMENT
CONTENT

FIG. 10

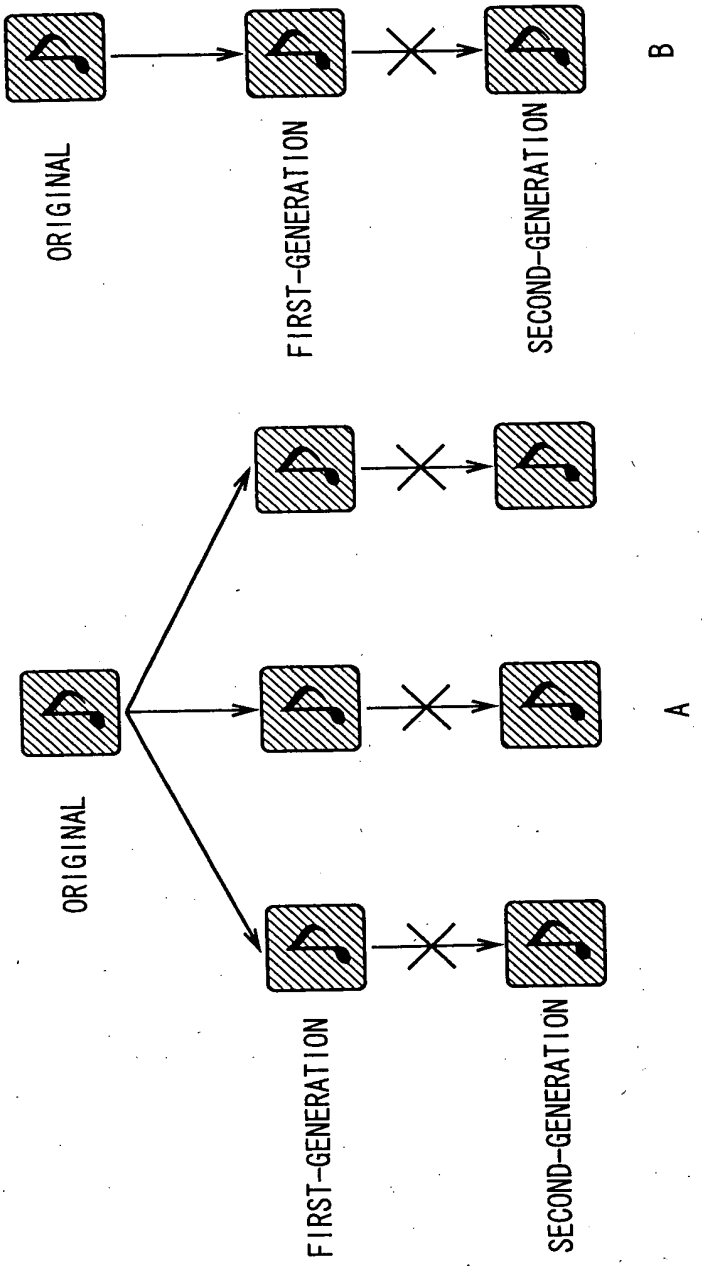

ORIGINAL
FIRST-GENERATION
SECOND-GENERATION
B
ORIGINAL
FIRST-GENERATION
SECOND-GENERATION
A

FIG.11

A

SERVICE CODE	INDICATION
0000h	NO CONDITION
0001h TO 00FFh	WITH CONDITIONS FOR EQUIPMENT
0100h TO 01FFh	WITH CONDITIONS FOR SEX
0200h TO 02FFh	WITH CONDITIONS FOR AGE
0300h TO 7FFFh	WITH OTHER CONDITIONS
8000h TO FFFFh	WITH CONDITIONS FOR USE POINT

B

CONDITION CODE	INDICATION
00h	NO CONDITION
01h	=
02h	≠
03h	< (SMALLER)
04h	> (LARGER)
05h	≦ (EQUAL OR SAMLLER)
06h	≧ (EQUAL OF LARGER)
07h TO FFh	FREE

FIG. 12

A

USER CONDITIONS 10	SERVICE CODE	VALUE CODE	CONDITION CODE
	80××h	0000C8h	06h
EQUIPMENT CONDITIONS 10	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h

USAGE CONDITIONS 10 OF UCPA

B

USER CONDITIONS 20	SERVICE CODE	VALUE CODE	CONDITION CODE
	80××h	0000C8h	03h
EQUIPMENT CONDITIONS 20	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h

USAGE CONDITIONS 20 OF UCPB

FIG. 13

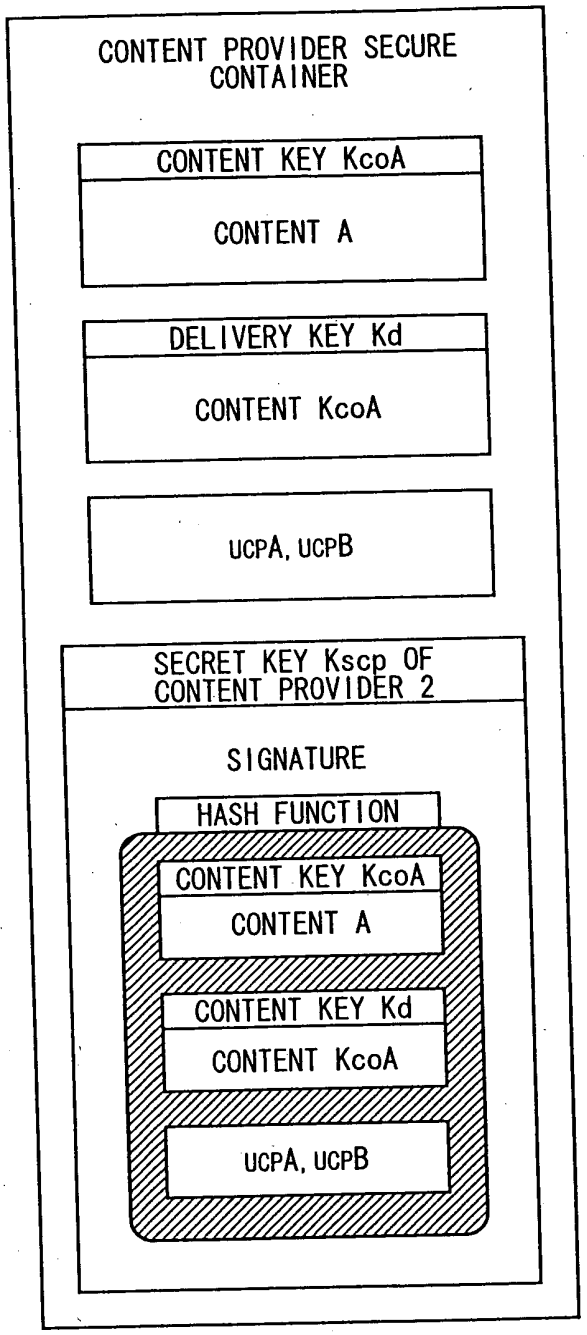

CONTENT PROVIDER SECURE CONTAINER
CONTENT KEY KcoA
CONTENT A
DELIVERY KEY Kd
CONTENT KcoA
UCPA, UCPB
SECRET KEY Kscp OF CONTENT PROVIDER 2
SIGNATURE
HASH FUNCTION
CONTENT KEY KcoA
CONTENT A
CONTENT KEY Kd
CONTENT KcoA
UCPA, UCPB

FIG. 14

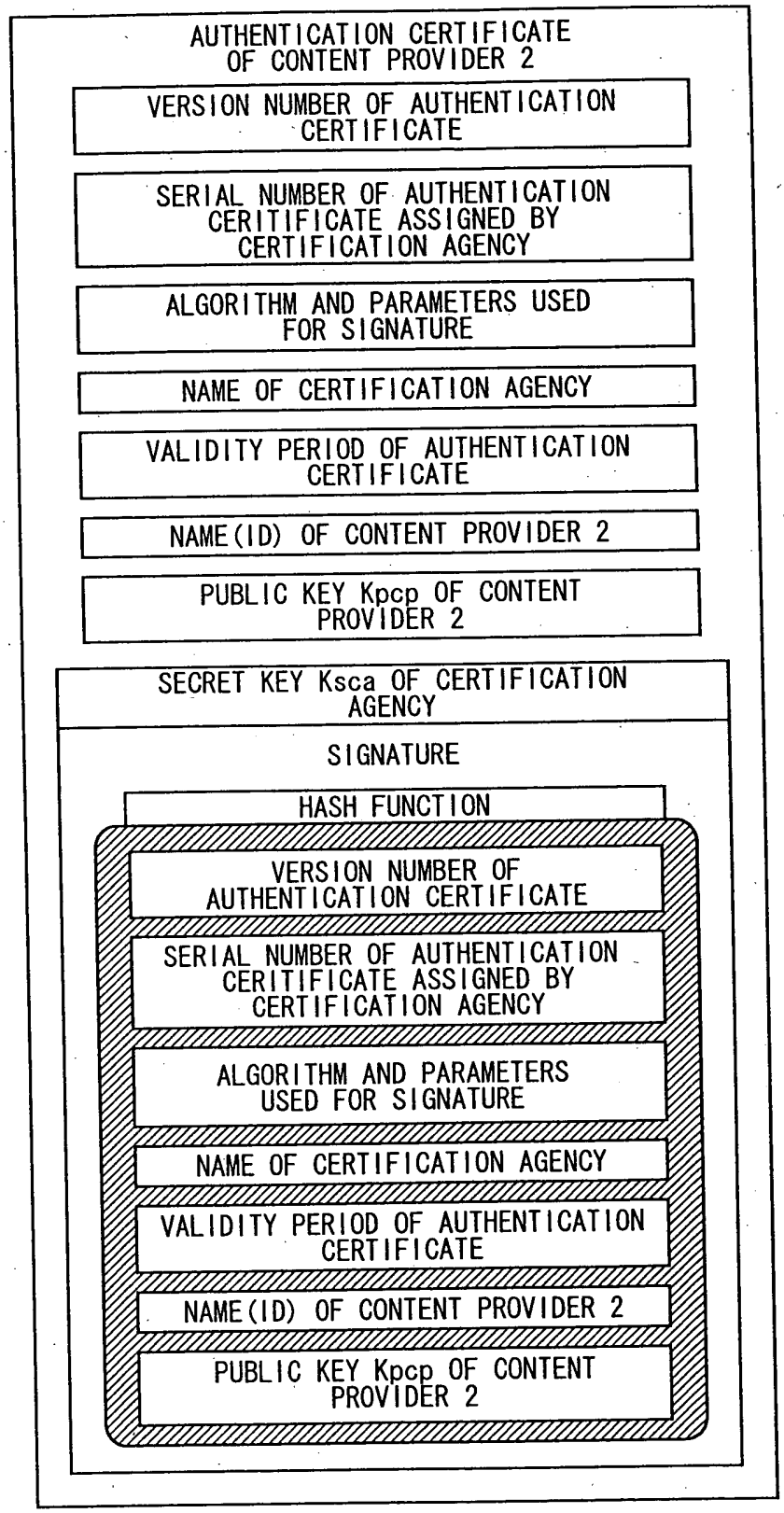

AUTHENTICATION CERTIFICATE OF CONTENT PROVIDER 2
VERSION NUMBER OF AUTHENTICATION CERTIFICATE
SERIAL NUMBER OF AUTHENTICATION CERITIFICATE ASSIGNED BY CERTIFICATION AGENCY
ALGORITHM AND PARAMETERS USED FOR SIGNATURE
NAME OF CERTIFICATION AGENCY
VALIDITY PERIOD OF AUTHENTICATION CERTIFICATE
NAME(ID) OF CONTENT PROVIDER 2
PUBLIC KEY Kpcp OF CONTENT PROVIDER 2
SECRET KEY Ksca OF CERTIFICATION AGENCY
SIGNATURE
HASH FUNCTION
VERSION NUMBER OF AUTHENTICATION CERTIFICATE
SERIAL NUMBER OF AUTHENTICATION CERITIFICATE ASSIGNED BY CERTIFICATION AGENCY
ALGORITHM AND PARAMETERS USED FOR SIGNATURE
NAME OF CERTIFICATION AGENCY
VALIDITY PERIOD OF AUTHENTICATION CERTIFICATE
NAME(ID) OF CONTENT PROVIDER 2
PUBLIC KEY Kpcp OF CONTENT PROVIDER 2

FIG. 15

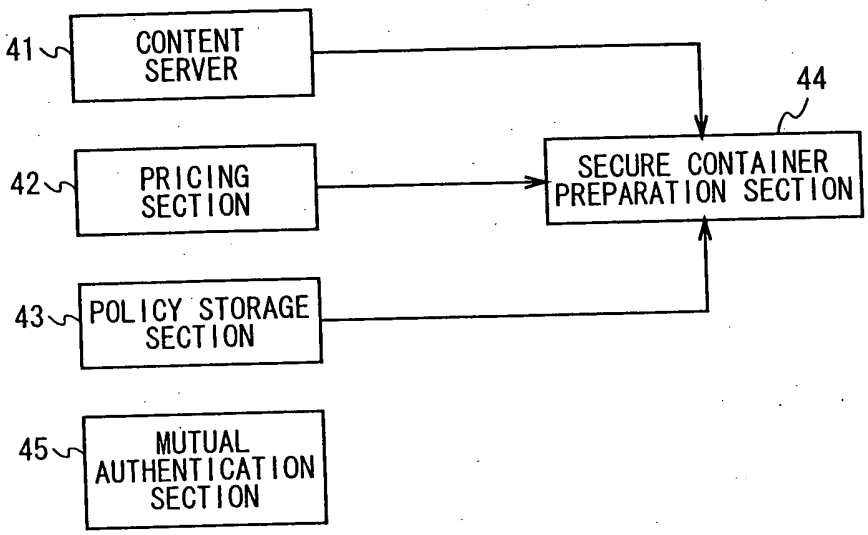

41
CONTENT SERVER
42
PRICING SECTION
43
POLICY STORAGE SECTION
45
MUTUAL AUTHENTICATION SECTION
44
SECURE CONTAINER PREPARATION SECTION
SERVICE PROVIDER 3

FIG. 16

CONTENT ID	ID OF CONTENT A	
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2	
UCP ID	ID OF UCP A	
UCP VALIDITY PERIOD	VALIDITY PERIOD OF UCPA	
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3	
PT ID	ID OF PTA-1	
PT VALIDITY PERIOD	VALIDITY PERIOD OF PTA-1	
PRICING CONDITIONS 10	USER CONDITIONS 10	MALE
	EQUIPMENT CONDITIONS 10	NO CONDITIONS
PRICE 11	2000YEN	
PRICE 12	600YEN	
PRICE 13	100YEN	
PRICE 14	300YEN	

PTA-1

CONTENT ID	ID OF CONTENT A	
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2	
UCP ID	ID OF UCP A	
UCP VALIDITY PERIOD	VALIDITY PERIOD OF UCPA	
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3	
PT ID	ID OF PTA-2	
PT VALIDITY PERIOD	VALIDITY PERIOD OF PTA-2	
PRICING CONDITIONS 20	USER CONDITIONS 20	FEMALE
	EQUIPMENT CONDITIONS 20	NO CONDITIONS
PRICE 21	1000YEN	
PRICE 22	300YEN	
PRICE 23	50YEN	
PRICE 24	150YEN	

PTA-2

FIG. 17

09/719015

A

USER CONDITIONS 10	SERVICE CODE	VALUE CODE	CONDITION CODE
	01××h	000000h	01h
EQUIPMENT CONDITIONS 10	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h

PRICING CONDITIONS 10 OF PTA-1

B

USER CONDITIONS 20	SERVICE CODE	VALUE CODE	CONDITION CODE
	01××h	000001h	01h
EQUIPMENT CONDITIONS 20	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h

PRICING CONDITIONS 20 OF PTA-2

FIG. 18

CONTENT ID	ID OF CONTENT A	
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2	
UCP ID	ID OF UCP B	
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3	
PT ID	ID OF PTB-1	
PT VALIDITY PERIOD	VALIDITY PERIOD OF PTB-1	
PRICING CONDITIONS 30	USER CONDITIONS 30	NO CONDITIONS
	EQUIPMENT CONDITIONS 30	SLAVE EQUIPMENT
PRICE 31	100YEN	
PRICE 32	300YEN	

PTB-1

A

CONTENT ID	ID OF CONTENT A	
CONTENT PROVIDER ID	ID OF CONTENT PROVIDER 2	
UCP ID	ID OF UCPB	
SERVICE PROVIDER ID	ID OF SERVICE PROVIDER 3	
PT ID	ID OF PTB-2	
PT VALIDITY PERIOD	VALIDITY PERIOD OF PTB-2	
PRICING CONDITIONS 40	USER CONDITIONS 40	NO CONDITIONS
	EQUIPMENT CONDITIONS 40	MASTER EQUIPMENT
PRICE 41	50YEN	
PRICE 42	150YEN	

PTB-2

B

FIG. 19

A

USER CONDITIONS 30	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h
EQUIPMENT CONDITIONS 30	SERVICE CODE	VALUE CODE	CONDITION CODE
	00××h	000064h	03h

PRICING CONDITIONS 30 OF PTB-1

B

USER CONDITIONS 40	SERVICE CODE	VALUE CODE	CONDITION CODE
	0000h	FFFFFFh	00h
EQUIPMENT CONDITIONS 40	SERVICE CODE	VALUE CODE	CONDITION CODE
	00××h	000064h	06h

PRICING CONDITIONS 40 OF PTB-2

FIG. 20

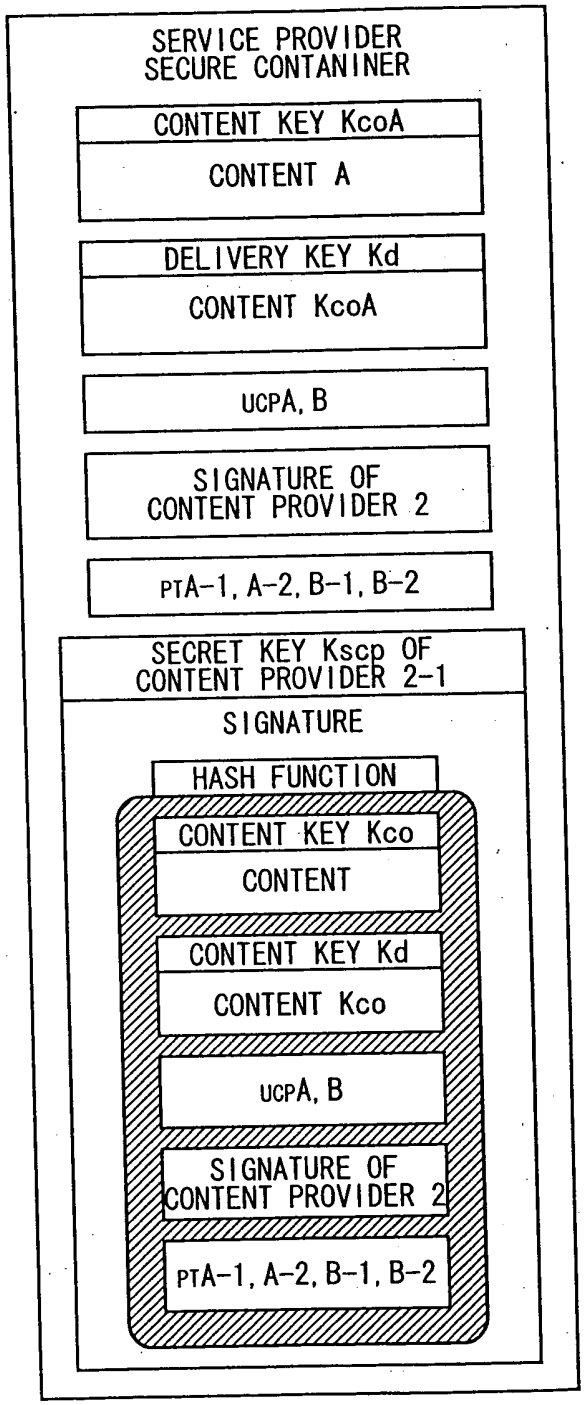

SERVICE PROVIDER
SECURE CONTANINER
CONTENT KEY KcoA
CONTENT A
DELIVERY KEY Kd
CONTENT KcoA
UCPA, B
SIGNATURE OF
CONTENT PROVIDER 2
PTA-1, A-2, B-1, B-2
SECRET KEY Kscp OF
CONTENT PROVIDER 2-1
SIGNATURE
HASH FUNCTION
CONTENT KEY Kco
CONTENT
CONTENT KEY Kd
CONTENT Kco
UCPA, B
SIGNATURE OF
CONTENT PROVIDER 2
PTA-1, A-2, B-1, B-2

FIG. 21

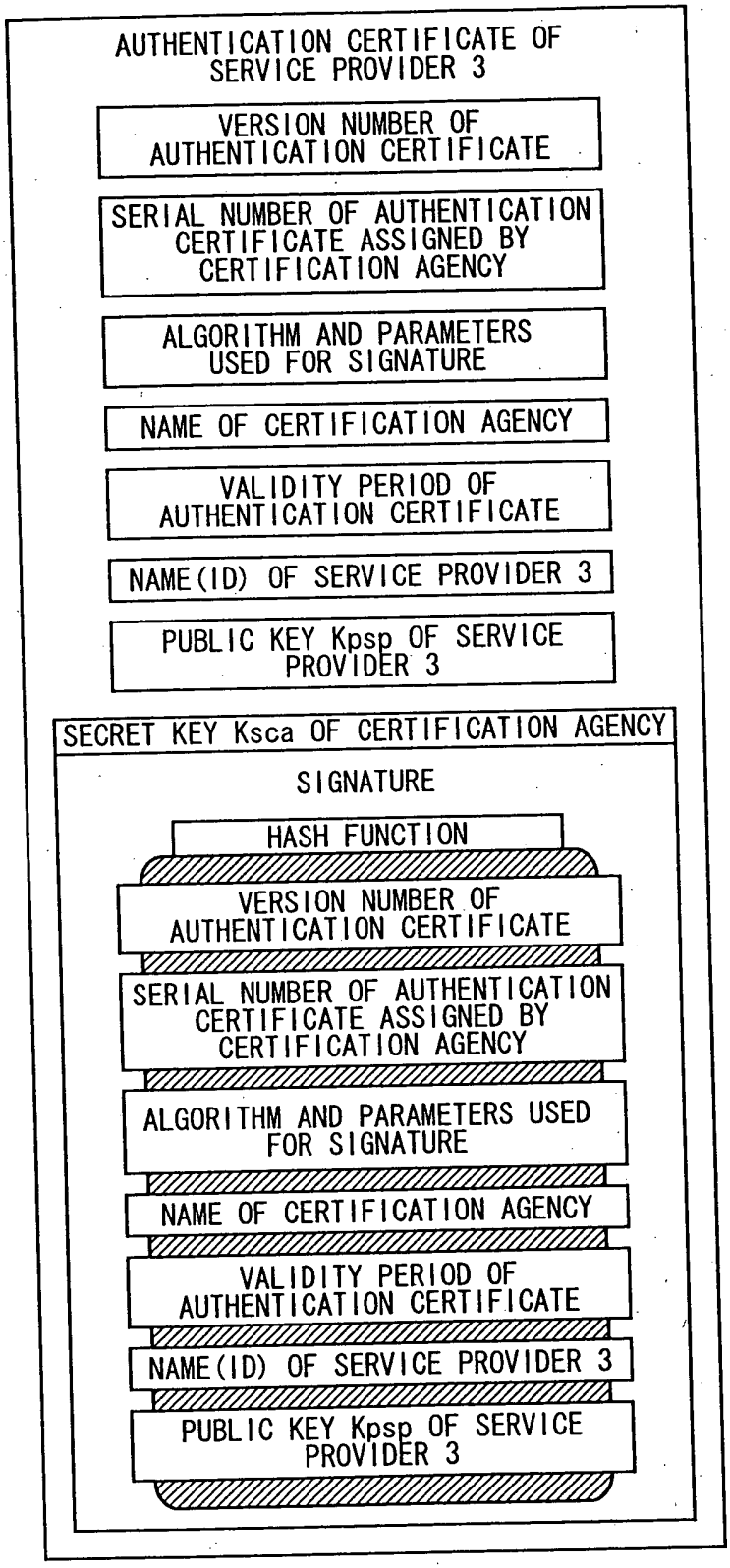

AUTHENTICATION CERTIFICATE OF SERVICE PROVIDER 3
VERSION NUMBER OF AUTHENTICATION CERTIFICATE
SERIAL NUMBER OF AUTHENTICATION CERTIFICATE ASSIGNED BY CERTIFICATION AGENCY
ALGORITHM AND PARAMETERS USED FOR SIGNATURE
NAME OF CERTIFICATION AGENCY
VALIDITY PERIOD OF AUTHENTICATION CERTIFICATE
NAME(ID) OF SERVICE PROVIDER 3
PUBLIC KEY Kpsp OF SERVICE PROVIDER 3
SECRET KEY Ksca OF CERTIFICATION AGENCY
SIGNATURE
HASH FUNCTION
VERSION NUMBER OF AUTHENTICATION CERTIFICATE
SERIAL NUMBER OF AUTHENTICATION CERTIFICATE ASSIGNED BY CERTIFICATION AGENCY
ALGORITHM AND PARAMETERS USED FOR SIGNATURE
NAME OF CERTIFICATION AGENCY
VALIDITY PERIOD OF AUTHENTICATION CERTIFICATE
NAME(ID) OF SERVICE PROVIDER 3
PUBLIC KEY Kpsp OF SERVICE PROVIDER 3

FIG. 22

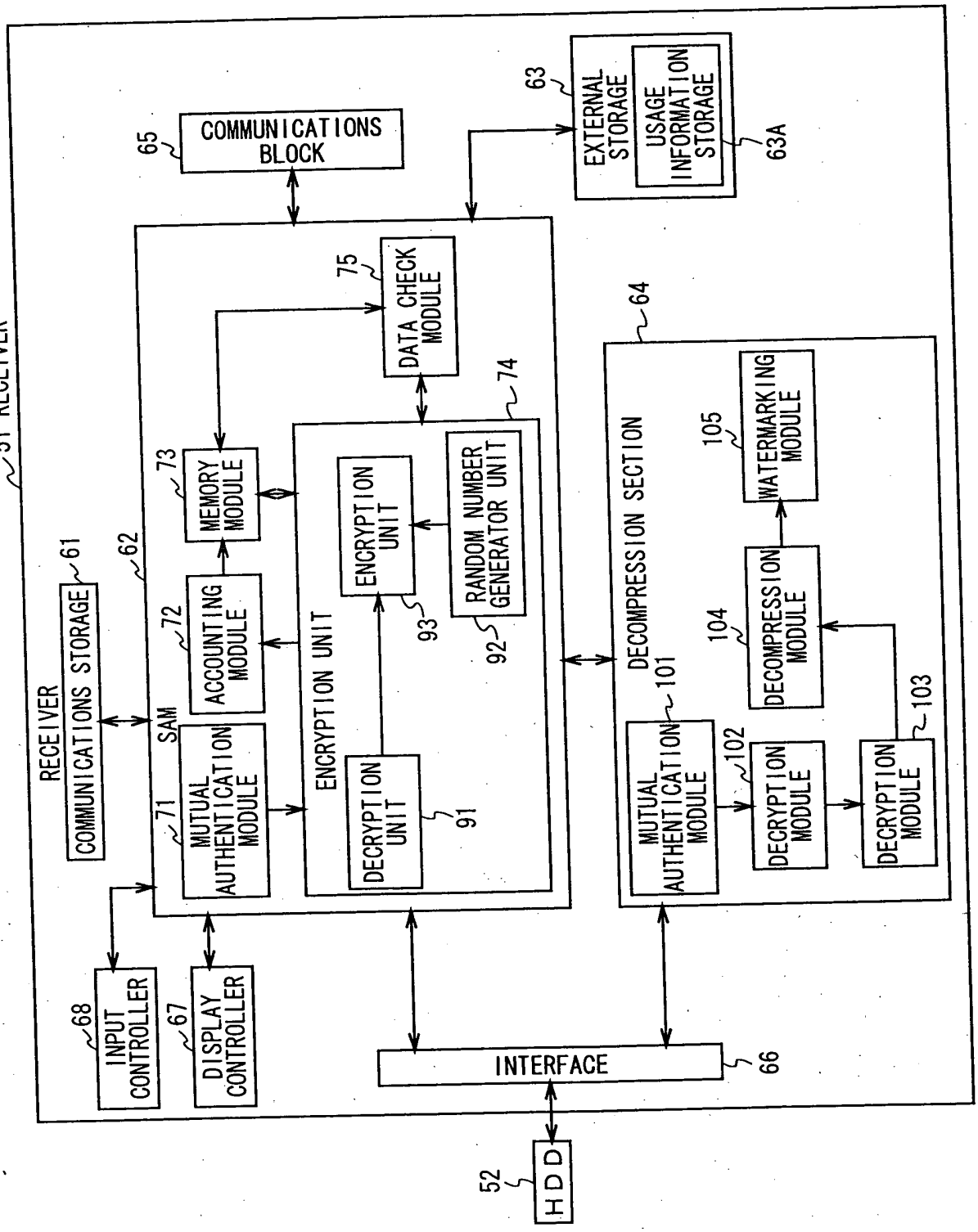

51 RECEIVER
65 COMMUNICATIONS BLOCK
63 EXTERNAL STORAGE
USAGE INFORMATION STORAGE
63A
75 DATA CHECK MODULE
64
74
73 MEMORY MODULE
62
61 RECEIVER COMMUNICATIONS STORAGE
72 ACCOUNTING MODULE
ENCRYPTION UNIT
ENCRYPTION UNIT
RANDOM NUMBER GENERATOR UNIT
93
92
DECOMPRESSION SECTION
105 WATERMARKING MODULE
104 DECOMPRESSION MODULE
SAM
71 MUTUAL AUTHENTICATION MODULE
DECRYPTION UNIT
91
101 MUTUAL AUTHENTICATION MODULE
102 DECRYPTION MODULE
103 DECRYPTION MODULE
68 INPUT CONTROLLER
67 DISPLAY CONTROLLER
INTERFACE
66
52 HDD

FIG. 23

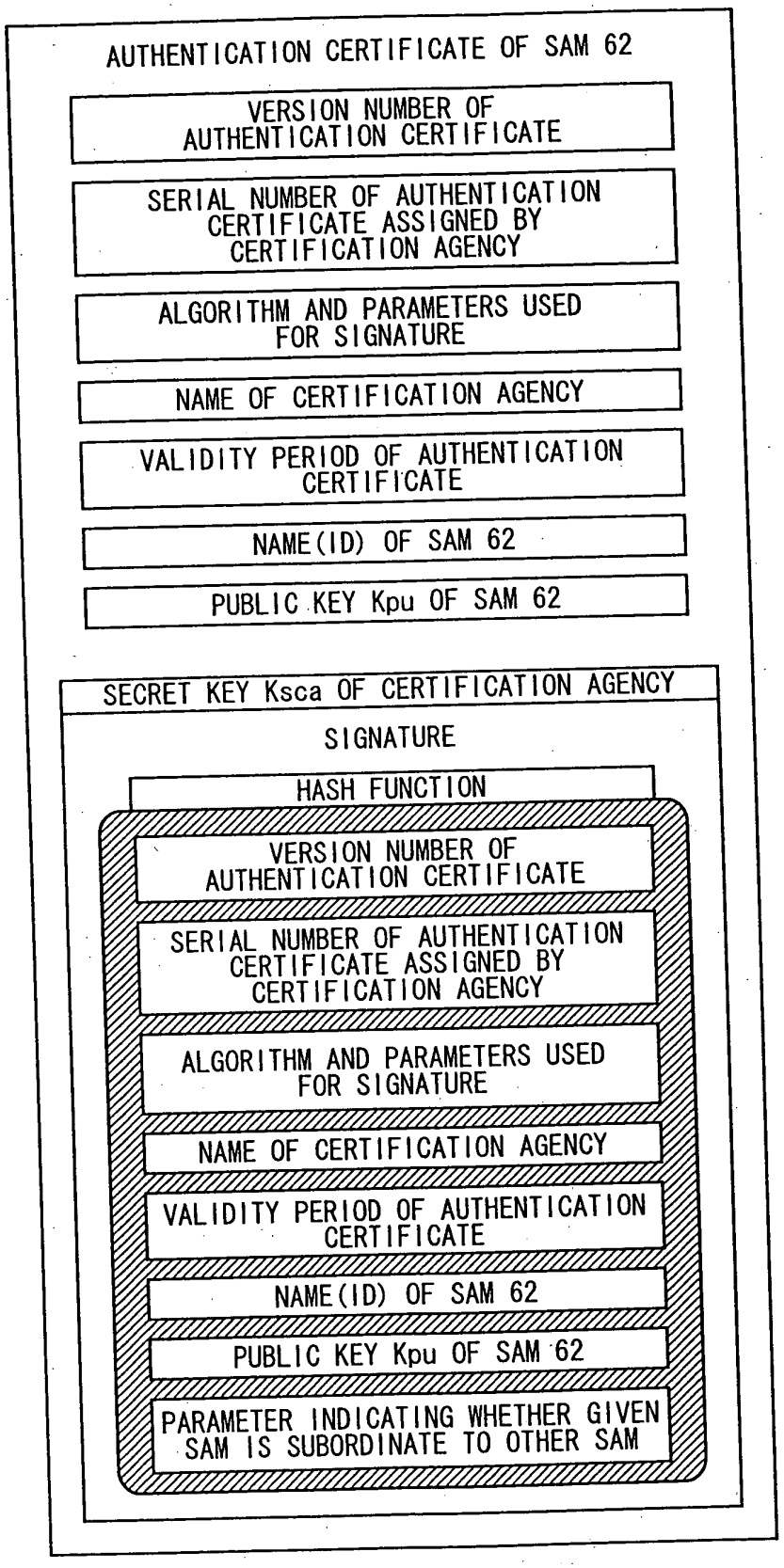

AUTHENTICATION CERTIFICATE OF SAM 62
VERSION NUMBER OF AUTHENTICATION CERTIFICATE
SERIAL NUMBER OF AUTHENTICATION CERTIFICATE ASSIGNED BY CERTIFICATION AGENCY
ALGORITHM AND PARAMETERS USED FOR SIGNATURE
NAME OF CERTIFICATION AGENCY
VALIDITY PERIOD OF AUTHENTICATION CERTIFICATE
NAME(ID) OF SAM 62
PUBLIC KEY Kpu OF SAM 62
SECRET KEY Ksca OF CERTIFICATION AGENCY
SIGNATURE
HASH FUNCTION
VERSION NUMBER OF AUTHENTICATION CERTIFICATE
SERIAL NUMBER OF AUTHENTICATION CERTIFICATE ASSIGNED BY CERTIFICATION AGENCY
ALGORITHM AND PARAMETERS USED FOR SIGNATURE
NAME OF CERTIFICATION AGENCY
VALIDITY PERIOD OF AUTHENTICATION CERTIFICATE
NAME(ID) OF SAM 62
PUBLIC KEY Kpu OF SAM 62
PARAMETER INDICATING WHETHER GIVEN SAM IS SUBORDINATE TO OTHER SAM

FIG. 24

CONTENT ID		ID OF CONTENT A
CONTENT PROVIDER ID		ID OF CONTENT PROVIDER 2
UCP ID		ID OF UCPA
UCP VALIDITY PERIOD		VALIDITY PERIOD OF UCPA
SERVICE PROVIDER ID		ID OF SERVICE PROVIDER 3
PT ID		ID OF PTA-1
PT VALIDITY PERIOD		VALIDITY PERIOD OF PTA-1
UCS ID		ID OF UCSA
SAM ID		ID OF SAM62
USER ID		ID OF USER F
USAGE DETAILS	ID	ID OF USAGE DETAILS 13
	TYPE	LIMITED-TIME REPRODUCTION
	PARAMETER	× × ×
	CONTROL TRANSFER STATUS	SOURCE:ID OF SAM62、DESTINATION:ID OF SAM62
USAGE HISTORY		× × ×

UCSA

FIG. 25

09/719015

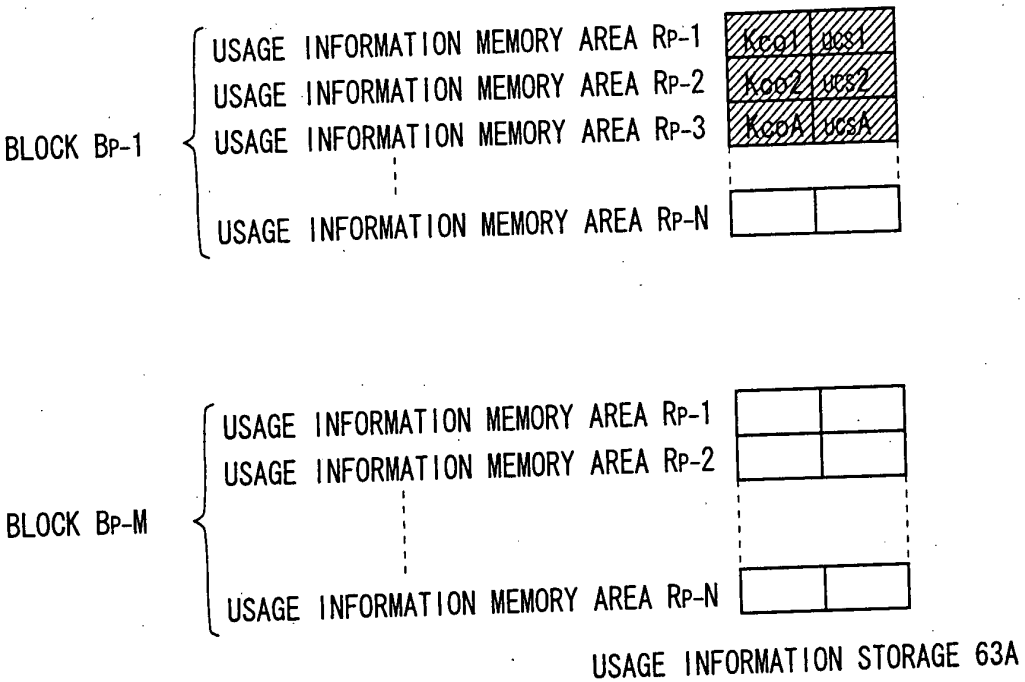


FIG. 26

CONTENT ID		ID OF CONTENT A
CONTENT PROVIDER ID		ID OF CONTENT PROVIDER 2
UCP ID		ID OF UCPA
UCP VALIDITY PERIOD		VALIDITY PERIOD OF UCPA
SERVICE PROVIDER ID		ID OF SERVICE PROVIDER 3
PT ID		ID OF PTA-1
PT VALIDITY PERIOD		VALIDITY PERIOD OF PTA-1
UCS ID		ID OF UCSA
SAM ID		ID OF SAM62
USER ID		ID OF USER F
USAGE DETAILS	ID	ID OF USAGE DETAILS 13
	TYPE	PURCHASE AND REPRODUCE
	PARAMETER	× × ×
	CONTROL TRANSFER STATUS	SOURCE:ID OF SAM62、DESTINATION:ID OF SAM62
ACCOUNTING HISTORY		× × ×

ACCOUNTING INFORMATION A

FIG. 27

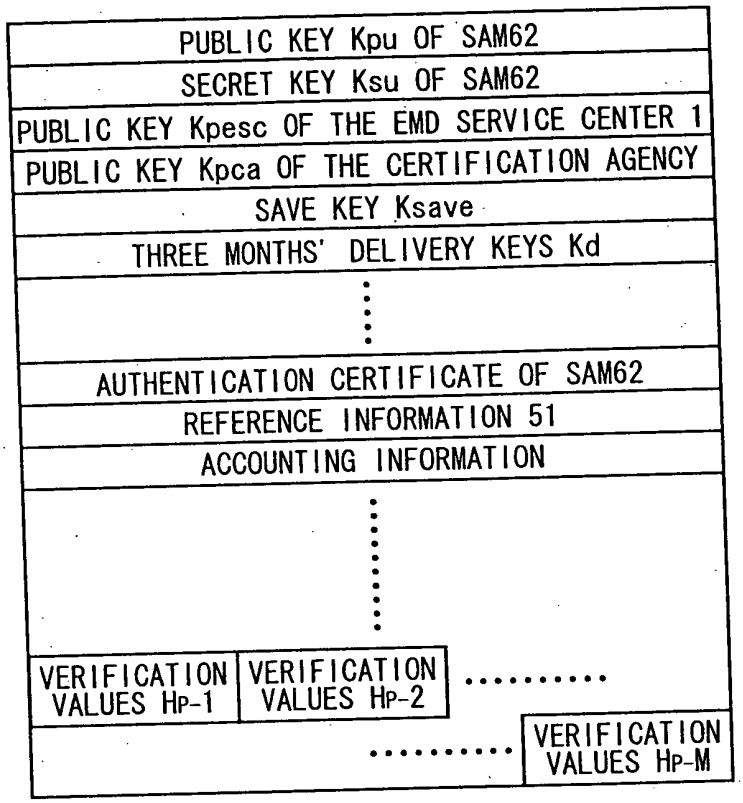

PUBLIC KEY Kpu OF SAM62
SECRET KEY Ksu OF SAM62
PUBLIC KEY Kpesc OF THE EMD SERVICE CENTER 1
PUBLIC KEY Kpca OF THE CERTIFICATION AGENCY
SAVE KEY Ksave
THREE MONTHS' DELIVERY KEYS Kd
AUTHENTICATION CERTIFICATE OF SAM62
REFERENCE INFORMATION 51
ACCOUNTING INFORMATION
VERIFICATION VALUES Hp-1
VERIFICATION VALUES Hp-2
VERIFICATION VALUES Hp-M

FIG. 28

SAM ID		ID OF SAM62
EQUIPMENT NUMBER		EQUIPMENT NUMBER(100) OF RECEIVERS 51
SETTLEMENT ID		SETTLEMENT ID OF USER
CHARGE LIMIT		FORMAL REGISTRATION
ACCOUNT-SETTLING USER INFORMATION	NAME	NAME OF USER
	ADDRESS	ADDRESS OF USER
	PHONE NUMBER	PHONE NUMBER OF USER
	SETTLEMENT INSTITUTION INFORMATION	SETTLEMENT INSTITUTION INFORMATION OF USER
	DATA OF BIRTH	DATE OF BIRTH OF USER
	AGE	AGE OF USER(21 YEARS)
	SEX	SEX OF USER(MALE)
	USER ID	USER ID OF USER
	PASSWORD	PASSWORD OF USER

USE POINT INFORMATION	USE POINF INFORMATION OF RECEIVERS 51

REFERENCE INFORMATION 51

FIG. 29

	SAM ID	USER ID	PURCHA-SING	ACCOUN-TING	EQUIPMENT BILLED	MASTER EQUIPMENT	STATUS FLAG	SIGNATURE TO CONDITIONS	SIGNATURE TO REGISTRATION LIST
REGISTRATION CONDITIONS OF RECEIVER 51	ID OF SAM62	USER ID	YES	YES	ID OF SAM62	NONE	NO RESTRI-CTION	××××	××××
REGISTRATION CONDITIONS OF RECEIVER 201	ID OF SAM212	USER ID	YES	NO	ID OF SAM62	NONE	NO RESTRI-CTION	××××	

LIST SECTION

SAM ID:ID OF SAM62 — ID OF SAM62

VALIDITY PERIOD — ××××

VERSION NUMBER — ××××

NUMBER OF EQUIPMENT CONNECTED — 2

SAM INFORMATION SECTION

REGISTRATION LIST OF RECEIVER 51

FIG. 30

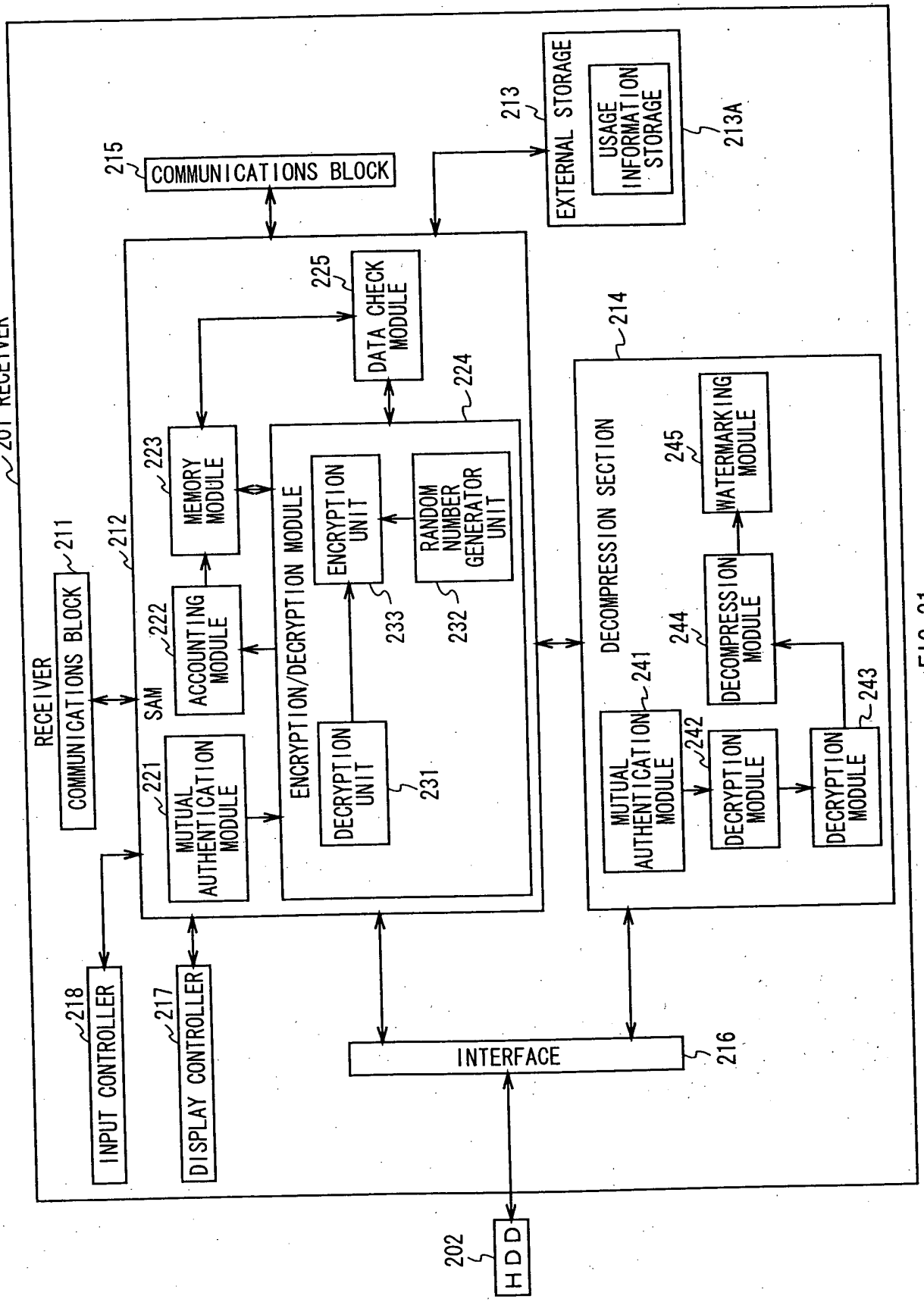

201 RECEIVER
215
COMMUNICATIONS BLOCK
213
EXTERNAL STORAGE
USAGE INFORMATION STORAGE
213A
225
DATA CHECK MODULE
224
214
DECOMPRESSION SECTION
245
WATERMARKING MODULE
223
MEMORY MODULE
ENCRYPTION/DECRYPTION MODULE
ENCRYPTION UNIT
RANDOM NUMBER GENERATOR UNIT
211
212
RECEIVER
COMMUNICATIONS BLOCK
SAM
222
ACCOUNTING MODULE
233
232
244
DECOMPRESSION MODULE
241
MUTUAL AUTHENTICATION MODULE
221
MUTUAL AUTHENTICATION MODULE
DECRYPTION UNIT
231
242
DECRYPTION MODULE
243
DECRYPTION MODULE
218
INPUT CONTROLLER
217
DISPLAY CONTROLLER
INTERFACE
216
202
HDD

FIG. 31

	SAM ID	USER ID	PURCHA-SING	ACCOUN-TING	EQUIPMENT BILLED	MASTER EQUIPMENT	STATUS FLAG	SIGNATURE TO CONDITIONS	SIGNATURE TO REGISTRATION LIST
REGISTRATION CONDITIONS OF RECEIVER 51	ID OF SAM62	USER ID	YES	YES	ID OF SAM62	NONE	NO RESTRI-CTION	××××	××××
REGISTRATION CONDITIONS OF RECEIVER 201	ID OF SAM212	USER ID	YES	NO	ID OF SAM62	NONE	NO RESTRI-CTION	××××	

LIST SECTION

SAM ID:ID OF SAM62 ID OF SAM212
VALIDITY PERIOD ××××
VERSION NUMBER ××××
NUMBER OF EQUIPMENT CONNECTED 2

SAM INFORMATION SECTION

REGISTRATION LIST OF RECEIVER 201

FIG. 32

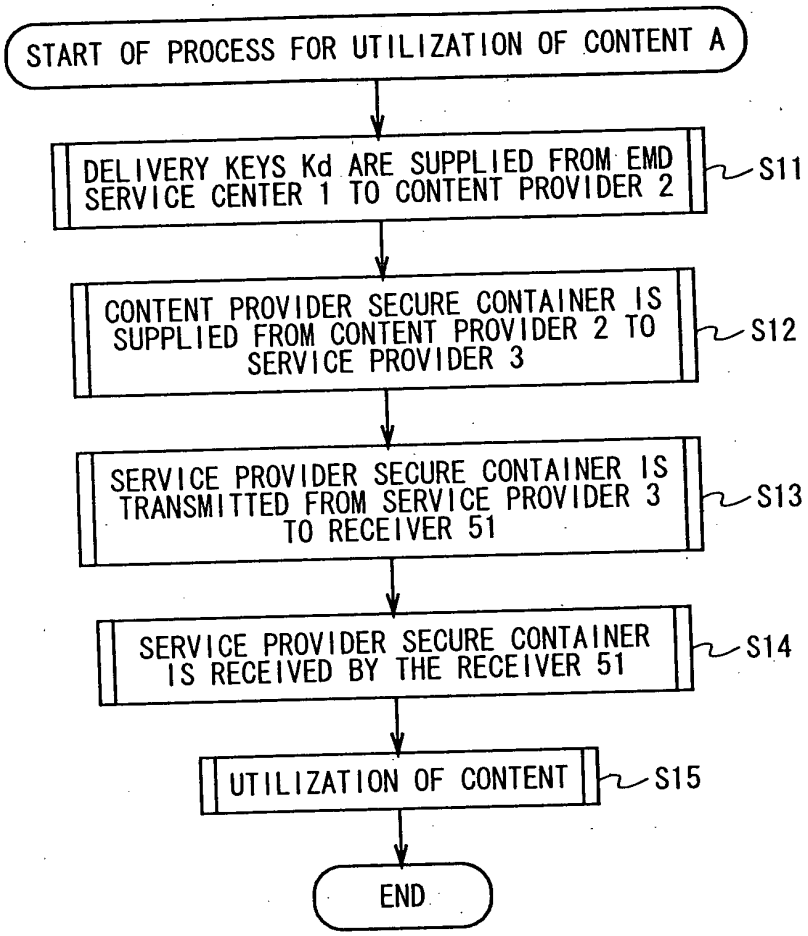

START OF PROCESS FOR UTILIZATION OF CONTENT A
DELIVERY KEYS Kd ARE SUPPLIED FROM EMD SERVICE CENTER 1 TO CONTENT PROVIDER 2
S11
CONTENT PROVIDER SECURE CONTAINER IS SUPPLIED FROM CONTENT PROVIDER 2 TO SERVICE PROVIDER 3
S12
SERVICE PROVIDER SECURE CONTAINER IS TRANSMITTED FROM SERVICE PROVIDER 3 TO RECEIVER 51
S13
SERVICE PROVIDER SECURE CONTAINER IS RECEIVED BY THE RECEIVER 51
S14
UTILIZATION OF CONTENT
S15
END

FIG. 33

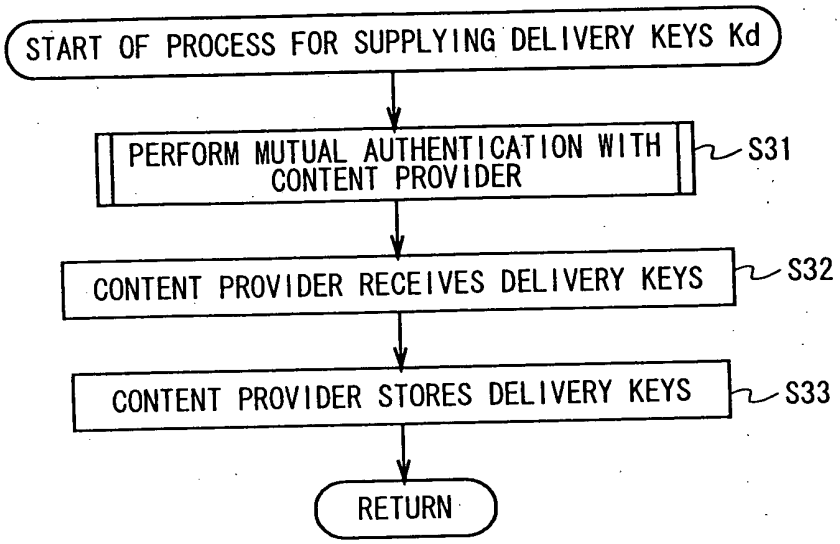

START OF PROCESS FOR SUPPLYING DELIVERY KEYS Kd
PERFORM MUTUAL AUTHENTICATION WITH CONTENT PROVIDER
S31
CONTENT PROVIDER RECEIVES DELIVERY KEYS
S32
CONTENT PROVIDER STORES DELIVERY KEYS
S33
RETURN

FIG. 34

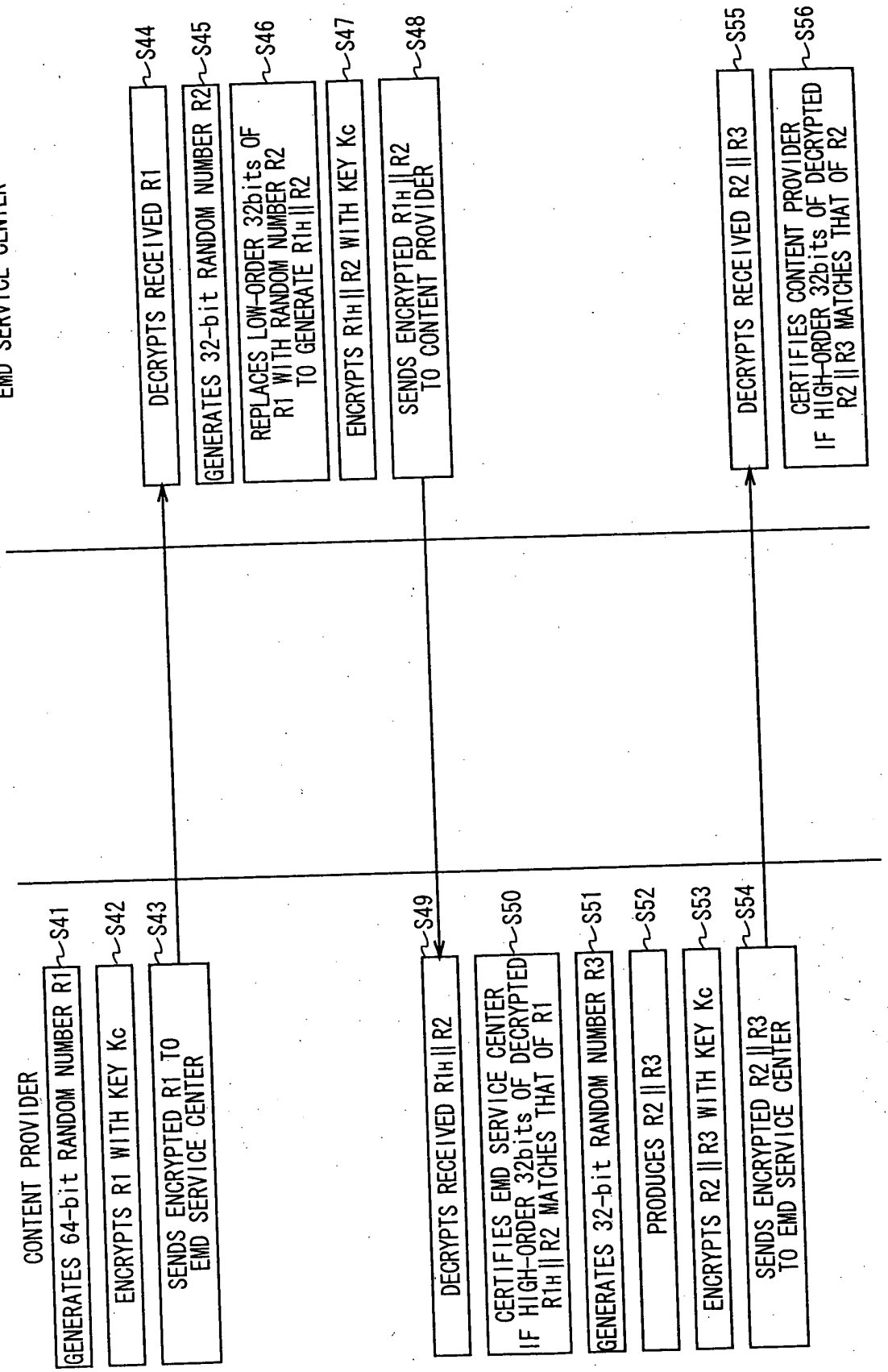

CONTENT PROVIDER
EMD SERVICE CENTER
GENERATES 64-bit RANDOM NUMBER R1
S41
ENCRYPTS R1 WITH KEY Kc
S42
SENDS ENCRYPTED R1 TO EMD SERVICE CENTER
S43
DECRYPTS RECEIVED R1
S44
GENERATES 32-bit RANDOM NUMBER R2
S45
REPLACES LOW-ORDER 32bits OF R1 WITH RANDOM NUMBER R2 TO GENERATE R1H || R2
S46
ENCRYPTS R1H || R2 WITH KEY Kc
S47
SENDS ENCRYPTED R1H || R2 TO CONTENT PROVIDER
S48
DECRYPTS RECEIVED R1H || R2
S49
CERTIFIES EMD SERVICE CENTER IF HIGH-ORDER 32bits OF DECRYPTED R1H || R2 MATCHES THAT OF R1
S50
GENERATES 32-bit RANDOM NUMBER R3
S51
PRODUCES R2 || R3
S52
ENCRYPTS R2 || R3 WITH KEY Kc
S53
SENDS ENCRYPTED R2 || R3 TO EMD SERVICE CENTER
S54
DECRYPTS RECEIVED R2 || R3
S55
CERTIFIES CONTENT PROVIDER IF HIGH-ORDER 32bits OF DECRYPTED R2 || R3 MATCHES THAT OF R2
S56

FIG. 35

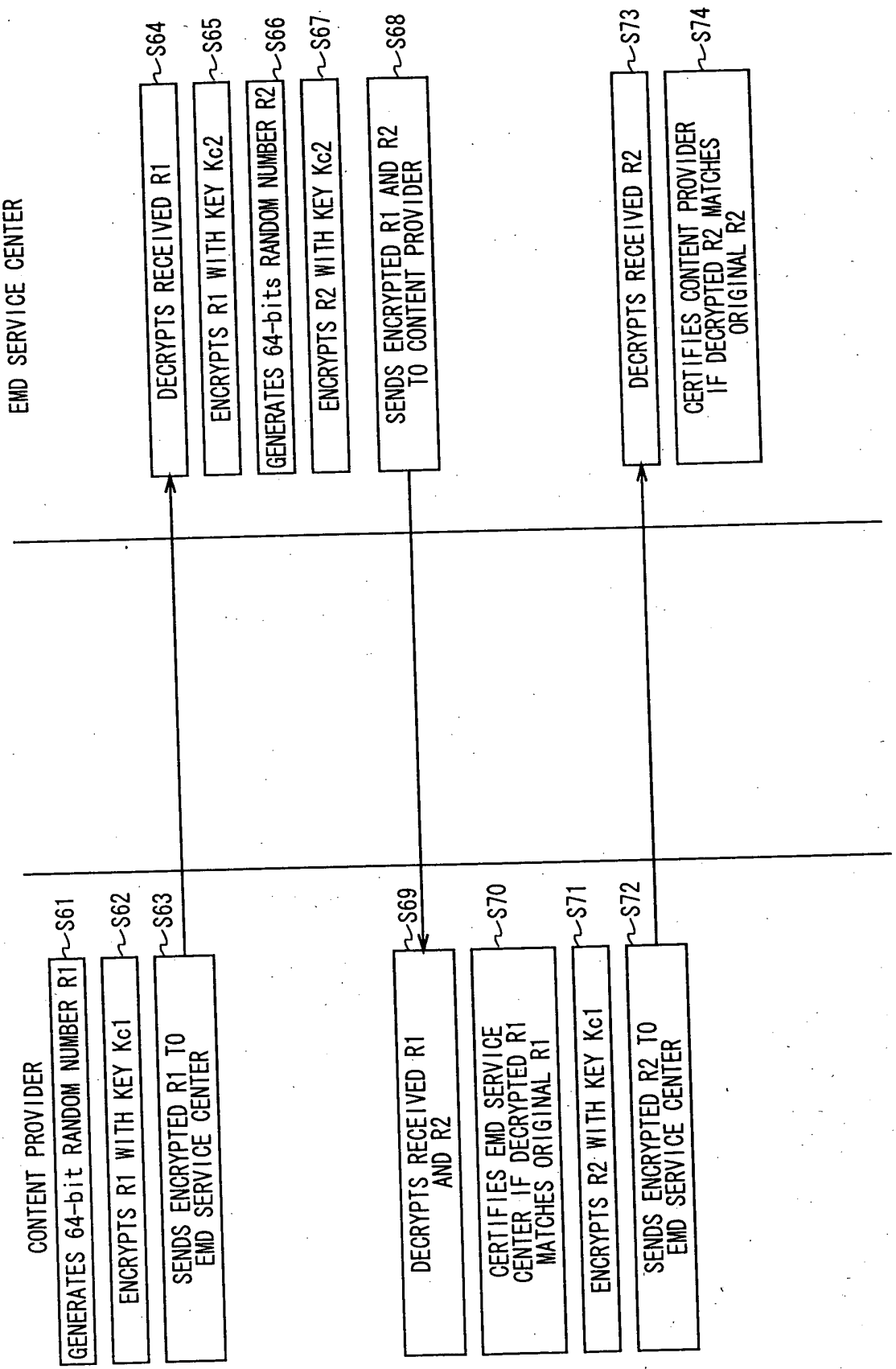

CONTENT PROVIDER
EMD SERVICE CENTER
GENERATES 64-bit RANDOM NUMBER R1
S61
ENCRYPTS R1 WITH KEY Kc1
S62
SENDS ENCRYPTED R1 TO EMD SERVICE CENTER
S63
DECRYPTS RECEIVED R1
S64
ENCRYPTS R1 WITH KEY Kc2
S65
GENERATES 64-bits RANDOM NUMBER R2
S66
ENCRYPTS R2 WITH KEY Kc2
S67
SENDS ENCRYPTED R1 AND R2 TO CONTENT PROVIDER
S68
DECRYPTS RECEIVED R1 AND R2
S69
CERTIFIES EMD SERVICE CENTER IF DECRYPTED R1 MATCHES ORIGINAL R1
S70
ENCRYPTS R2 WITH KEY Kc1
S71
SENDS ENCRYPTED R2 TO EMD SERVICE CENTER
S72
DECRYPTS RECEIVED R2
S73
CERTIFIES CONTENT PROVIDER IF DECRYPTED R2 MATCHES ORIGINAL R2
S74

FIG. 36

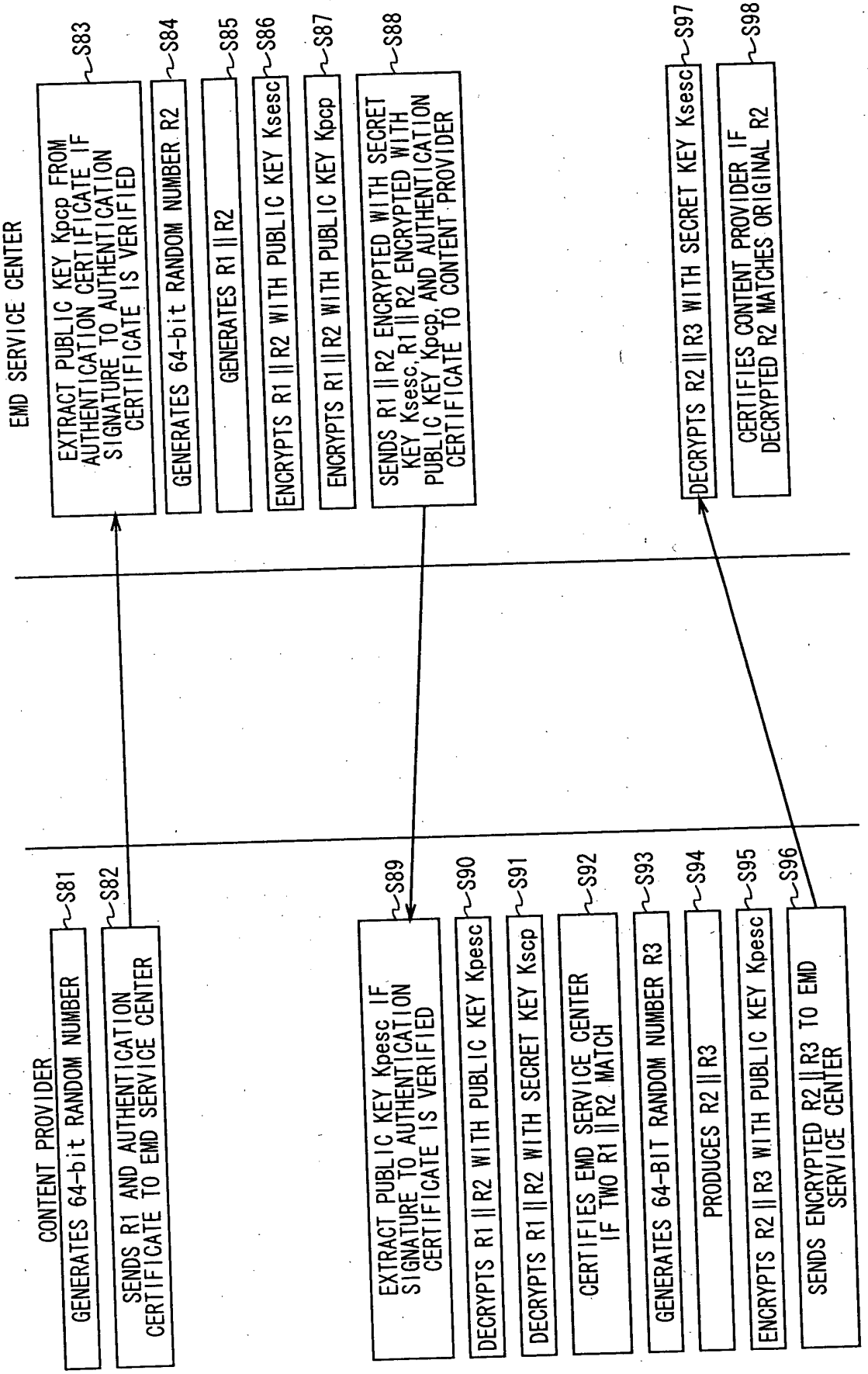

CONTENT PROVIDER
EMD SERVICE CENTER
GENERATES 64-bit RANDOM NUMBER
S81
SENDS R1 AND AUTHENTICATION CERTIFICATE TO EMD SERVICE CENTER
S82
EXTRACT PUBLIC KEY Kpcp FROM AUTHENTICATION CERTIFICATE IF SIGNATURE TO AUTHENTICATION CERTIFICATE IS VERIFIED
S83
GENERATES 64-bit RANDOM NUMBER R2
S84
GENERATES R1 || R2
S85
ENCRYPTS R1 || R2 WITH PUBLIC KEY Ksesc
S86
ENCRYPTS R1 || R2 WITH PUBLIC KEY Kpcp
S87
SENDS R1 || R2 ENCRYPTED WITH SECRET KEY Ksesc, R1 || R2 ENCRYPTED WITH PUBLIC KEY Kpcp, AND AUTHENTICATION CERTIFICATE TO CONTENT PROVIDER
S88
EXTRACT PUBLIC KEY Kpesc IF SIGNATURE TO AUTHENTICATION CERTIFICATE IS VERIFIED
S89
DECRYPTS R1 || R2 WITH PUBLIC KEY Kpesc
S90
DECRYPTS R1 || R2 WITH SECRET KEY Kscp
S91
CERTIFIES EMD SERVICE CENTER IF TWO R1 || R2 MATCH
S92
GENERATES 64-BIT RANDOM NUMBER R3
S93
PRODUCES R2 || R3
S94
ENCRYPTS R2 || R3 WITH PUBLIC KEY Kpesc
S95
SENDS ENCRYPTED R2 || R3 TO EMD SERVICE CENTER
S96
DECRYPTS R2 || R3 WITH SECRET KEY Ksesc
S97
CERTIFIES CONTENT PROVIDER IF DECRYPTED R2 MATCHES ORIGINAL R2
S98

FIG. 37

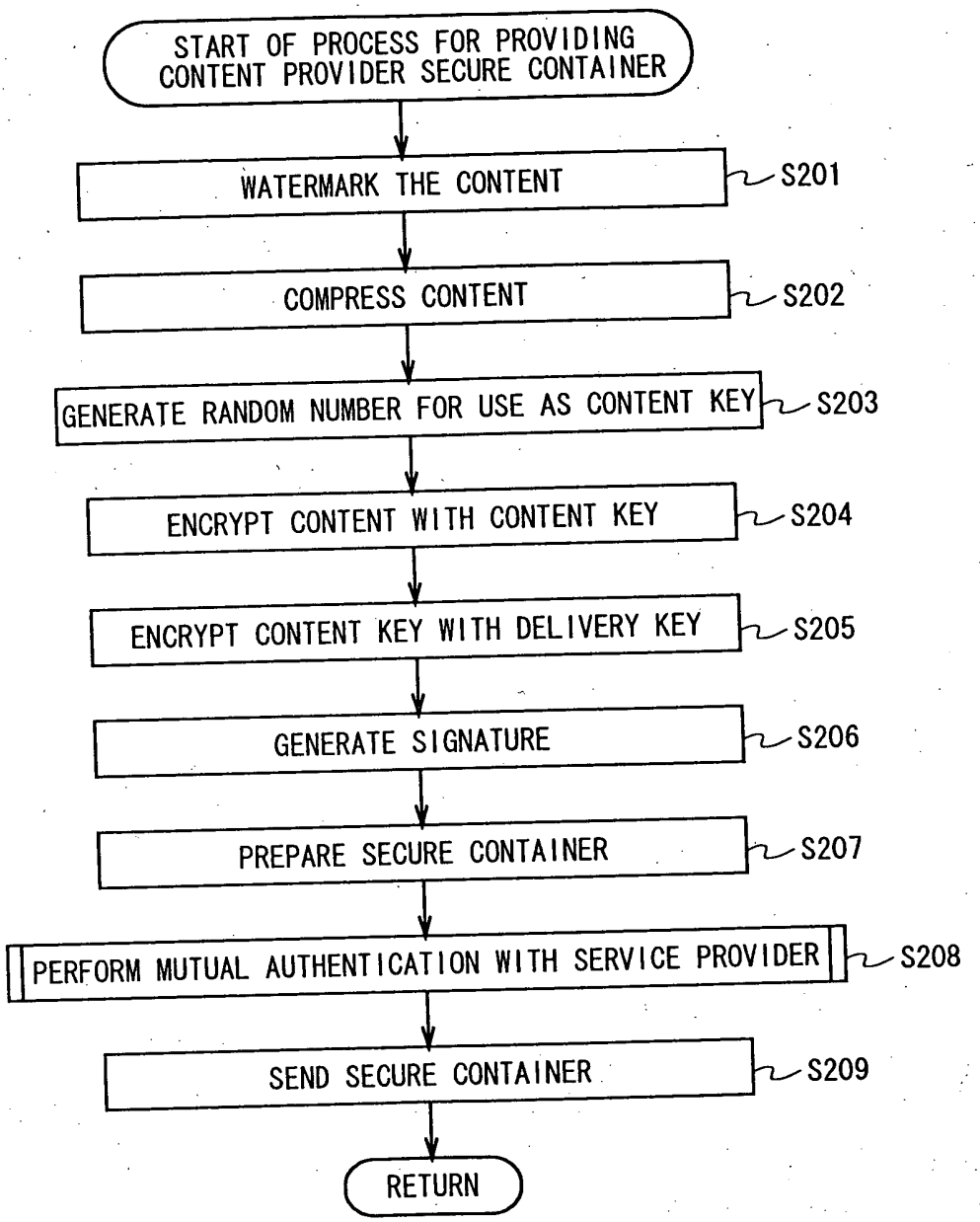

START OF PROCESS FOR PROVIDING CONTENT PROVIDER SECURE CONTAINER
WATERMARK THE CONTENT
S201
COMPRESS CONTENT
S202
GENERATE RANDOM NUMBER FOR USE AS CONTENT KEY
S203
ENCRYPT CONTENT WITH CONTENT KEY
S204
ENCRYPT CONTENT KEY WITH DELIVERY KEY
S205
GENERATE SIGNATURE
S206
PREPARE SECURE CONTAINER
S207
PERFORM MUTUAL AUTHENTICATION WITH SERVICE PROVIDER
S208
SEND SECURE CONTAINER
S209
RETURN

FIG. 38

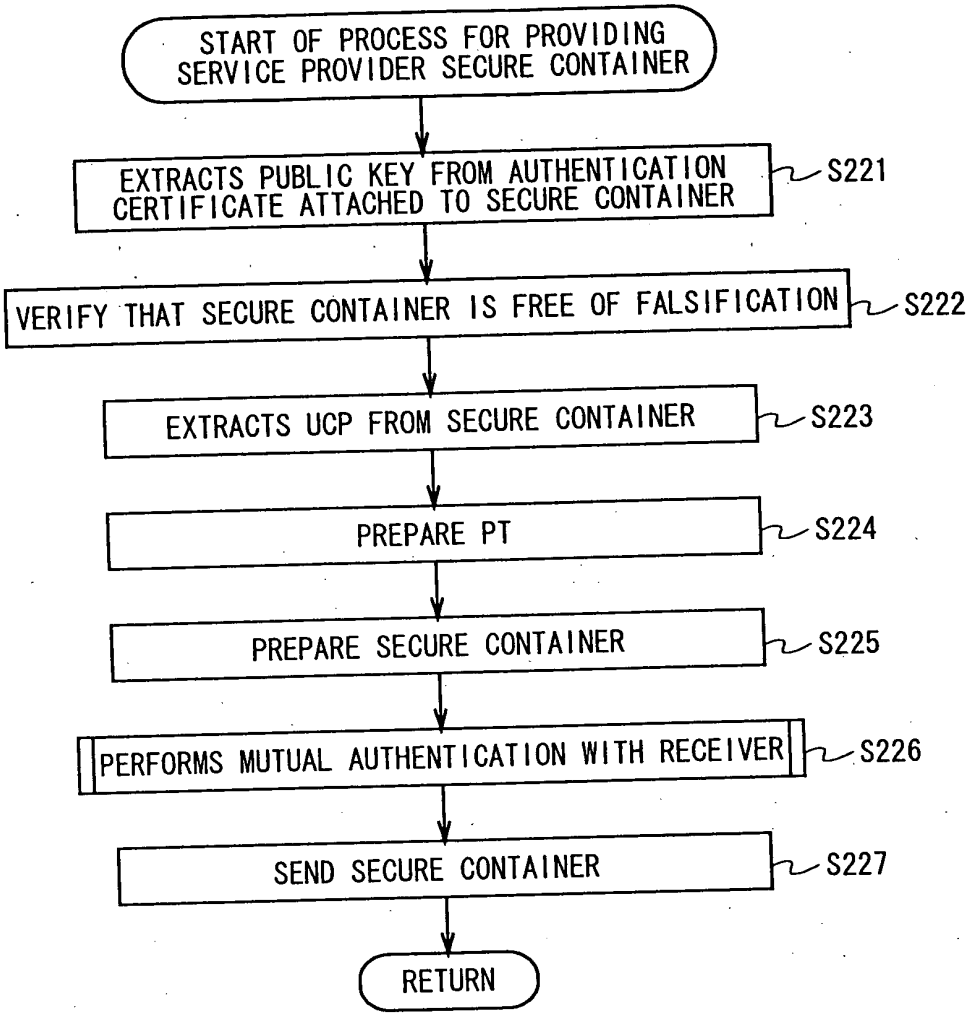

START OF PROCESS FOR PROVIDING SERVICE PROVIDER SECURE CONTAINER
EXTRACTS PUBLIC KEY FROM AUTHENTICATION CERTIFICATE ATTACHED TO SECURE CONTAINER
S221
VERIFY THAT SECURE CONTAINER IS FREE OF FALSIFICATION
S222
EXTRACTS UCP FROM SECURE CONTAINER
S223
PREPARE PT
S224
PREPARE SECURE CONTAINER
S225
PERFORMS MUTUAL AUTHENTICATION WITH RECEIVER
S226
SEND SECURE CONTAINER
S227
RETURN

FIG. 39

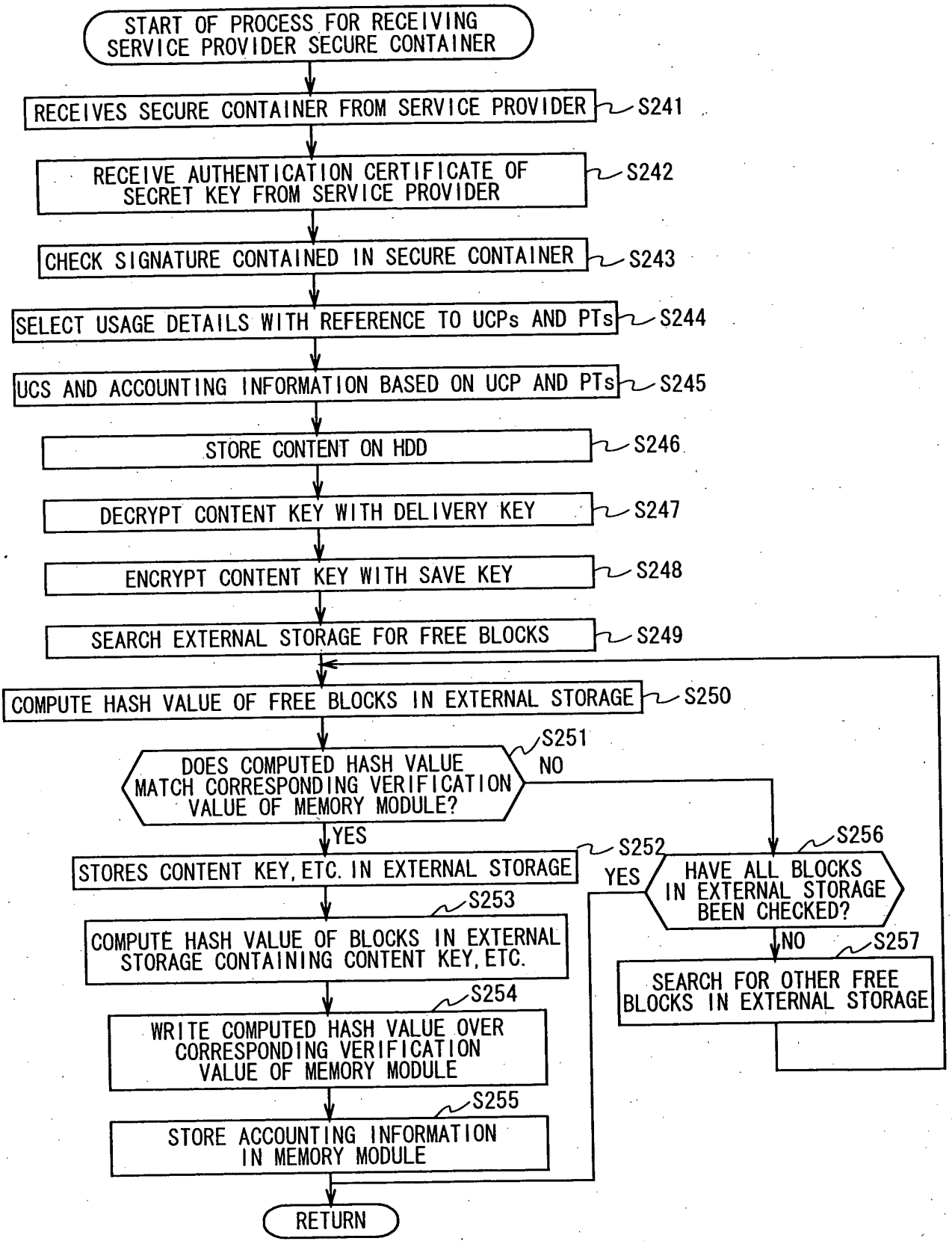

START OF PROCESS FOR RECEIVING SERVICE PROVIDER SECURE CONTAINER
RECEIVES SECURE CONTAINER FROM SERVICE PROVIDER
S241
RECEIVE AUTHENTICATION CERTIFICATE OF SECRET KEY FROM SERVICE PROVIDER
S242
CHECK SIGNATURE CONTAINED IN SECURE CONTAINER
S243
SELECT USAGE DETAILS WITH REFERENCE TO UCPs AND PTs
S244
UCS AND ACCOUNTING INFORMATION BASED ON UCP AND PTs
S245
STORE CONTENT ON HDD
S246
DECRYPT CONTENT KEY WITH DELIVERY KEY
S247
ENCRYPT CONTENT KEY WITH SAVE KEY
S248
SEARCH EXTERNAL STORAGE FOR FREE BLOCKS
S249
COMPUTE HASH VALUE OF FREE BLOCKS IN EXTERNAL STORAGE
S250
DOES COMPUTED HASH VALUE MATCH CORRESPONDING VERIFICATION VALUE OF MEMORY MODULE?
S251
NO
YES
STORES CONTENT KEY, ETC. IN EXTERNAL STORAGE
S252
COMPUTE HASH VALUE OF BLOCKS IN EXTERNAL STORAGE CONTAINING CONTENT KEY, ETC.
S253
WRITE COMPUTED HASH VALUE OVER CORRESPONDING VERIFICATION VALUE OF MEMORY MODULE
S254
STORE ACCOUNTING INFORMATION IN MEMORY MODULE
S255
RETURN
HAVE ALL BLOCKS IN EXTERNAL STORAGE BEEN CHECKED?
S256
YES
NO
SEARCH FOR OTHER FREE BLOCKS IN EXTERNAL STORAGE
S257

FIG. 40

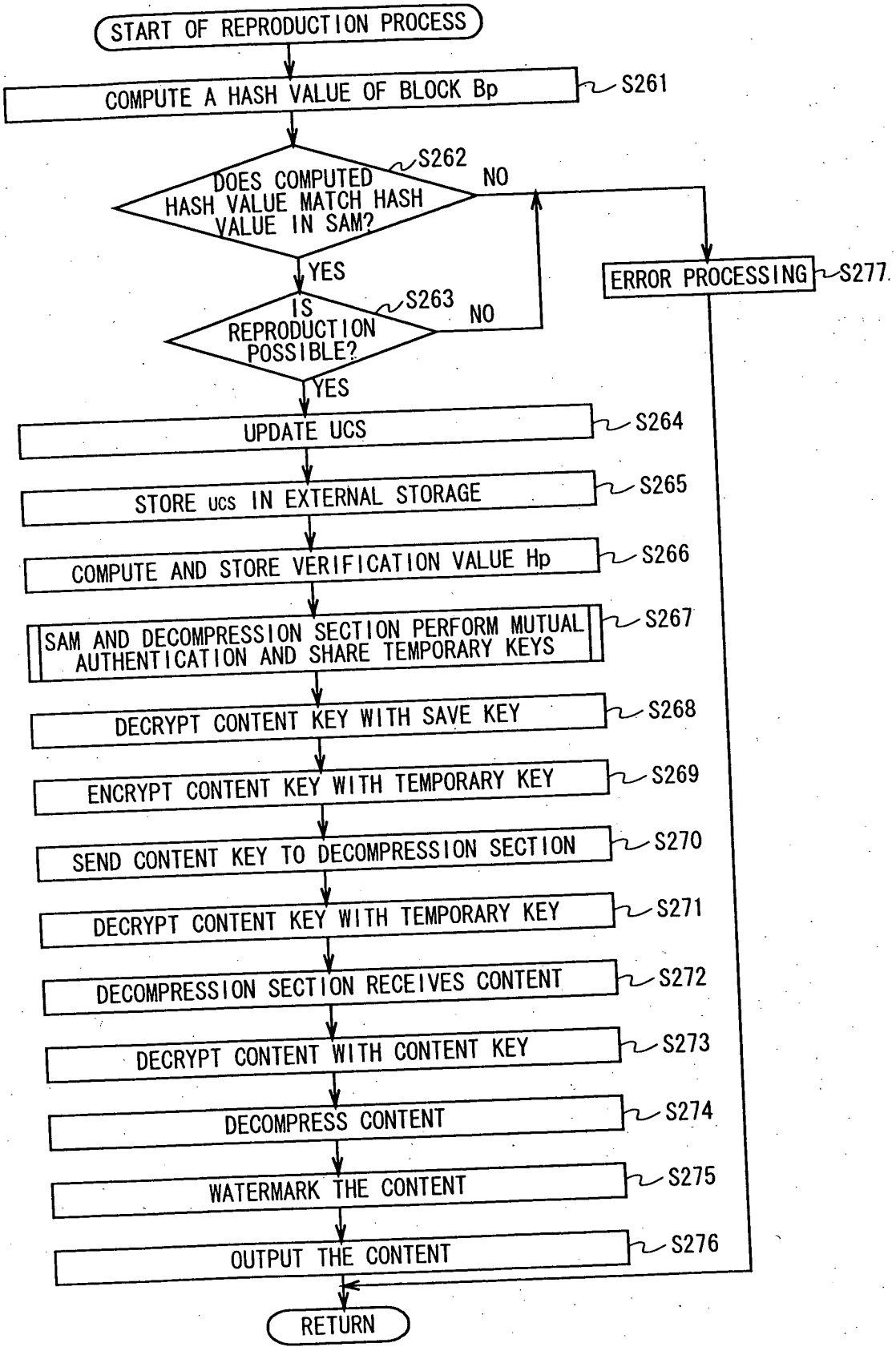

START OF REPRODUCTION PROCESS
COMPUTE A HASH VALUE OF BLOCK Bp
S261
DOES COMPUTED HASH VALUE MATCH HASH VALUE IN SAM?
S262
NO
YES
ERROR PROCESSING
S277
IS REPRODUCTION POSSIBLE?
S263
NO
YES
UPDATE UCS
S264
STORE ucs IN EXTERNAL STORAGE
S265
COMPUTE AND STORE VERIFICATION VALUE Hp
S266
SAM AND DECOMPRESSION SECTION PERFORM MUTUAL AUTHENTICATION AND SHARE TEMPORARY KEYS
S267
DECRYPT CONTENT KEY WITH SAVE KEY
S268
ENCRYPT CONTENT KEY WITH TEMPORARY KEY
S269
SEND CONTENT KEY TO DECOMPRESSION SECTION
S270
DECRYPT CONTENT KEY WITH TEMPORARY KEY
S271
DECOMPRESSION SECTION RECEIVES CONTENT
S272
DECRYPT CONTENT WITH CONTENT KEY
S273
DECOMPRESS CONTENT
S274
WATERMARK THE CONTENT
S275
OUTPUT THE CONTENT
S276
RETURN

FIG. 41

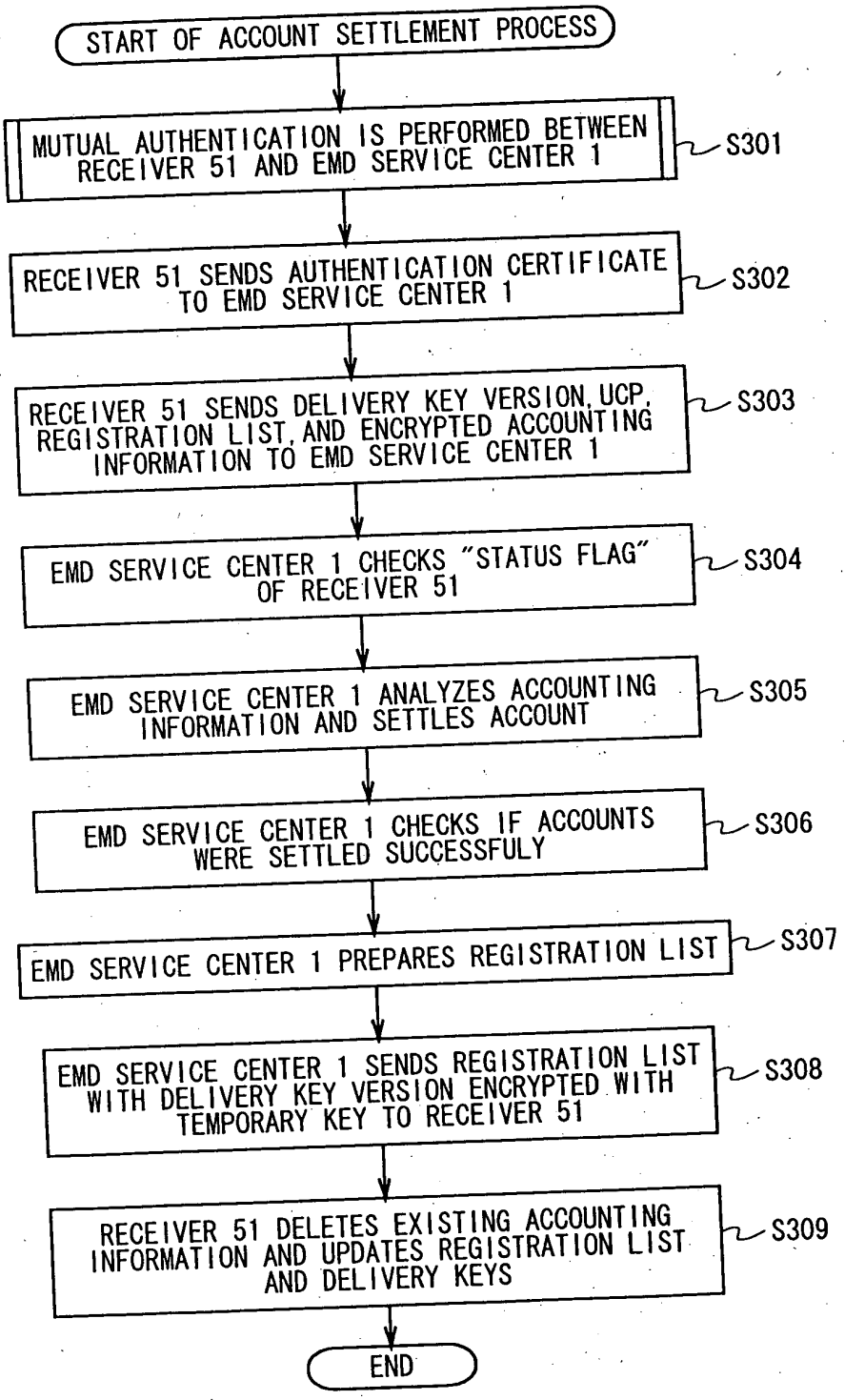

START OF ACCOUNT SETTLEMENT PROCESS
MUTUAL AUTHENTICATION IS PERFORMED BETWEEN RECEIVER 51 AND EMD SERVICE CENTER 1
S301
RECEIVER 51 SENDS AUTHENTICATION CERTIFICATE TO EMD SERVICE CENTER 1
S302
RECEIVER 51 SENDS DELIVERY KEY VERSION, UCP, REGISTRATION LIST, AND ENCRYPTED ACCOUNTING INFORMATION TO EMD SERVICE CENTER 1
S303
EMD SERVICE CENTER 1 CHECKS "STATUS FLAG" OF RECEIVER 51
S304
EMD SERVICE CENTER 1 ANALYZES ACCOUNTING INFORMATION AND SETTLES ACCOUNT
S305
EMD SERVICE CENTER 1 CHECKS IF ACCOUNTS WERE SETTLED SUCCESSFULY
S306
EMD SERVICE CENTER 1 PREPARES REGISTRATION LIST
S307
EMD SERVICE CENTER 1 SENDS REGISTRATION LIST WITH DELIVERY KEY VERSION ENCRYPTED WITH TEMPORARY KEY TO RECEIVER 51
S308
RECEIVER 51 DELETES EXISTING ACCOUNTING INFORMATION AND UPDATES REGISTRATION LIST AND DELIVERY KEYS
S309
END

FIG. 42

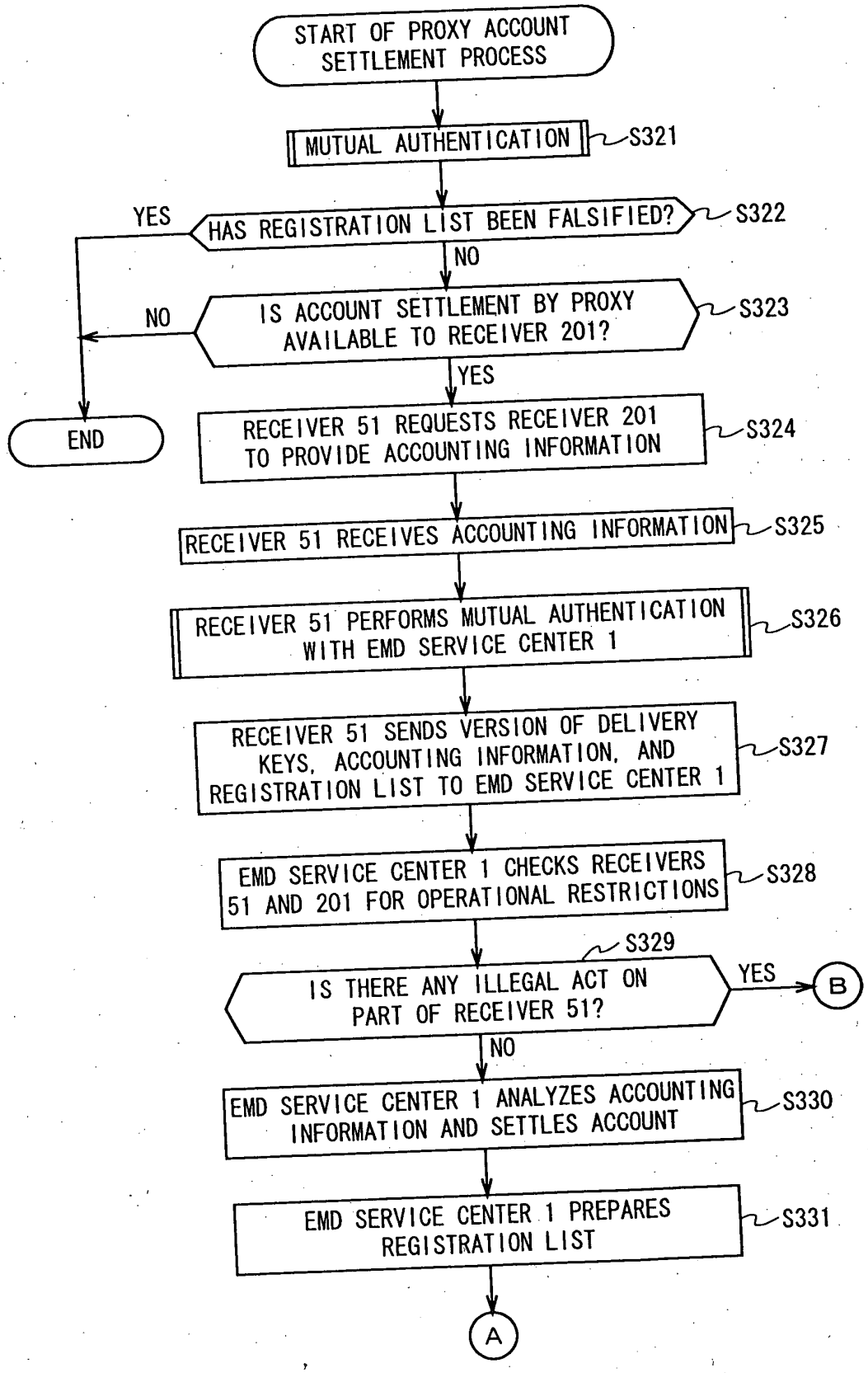

START OF PROXY ACCOUNT SETTLEMENT PROCESS
MUTUAL AUTHENTICATION
S321
HAS REGISTRATION LIST BEEN FALSIFIED?
S322
YES
NO
IS ACCOUNT SETTLEMENT BY PROXY AVAILABLE TO RECEIVER 201?
S323
NO
YES
END
RECEIVER 51 REQUESTS RECEIVER 201 TO PROVIDE ACCOUNTING INFORMATION
S324
RECEIVER 51 RECEIVES ACCOUNTING INFORMATION
S325
RECEIVER 51 PERFORMS MUTUAL AUTHENTICATION WITH EMD SERVICE CENTER 1
S326
RECEIVER 51 SENDS VERSION OF DELIVERY KEYS, ACCOUNTING INFORMATION, AND REGISTRATION LIST TO EMD SERVICE CENTER 1
S327
EMD SERVICE CENTER 1 CHECKS RECEIVERS 51 AND 201 FOR OPERATIONAL RESTRICTIONS
S328
S329
IS THERE ANY ILLEGAL ACT ON PART OF RECEIVER 51?
YES
B
NO
EMD SERVICE CENTER 1 ANALYZES ACCOUNTING INFORMATION AND SETTLES ACCOUNT
S330
EMD SERVICE CENTER 1 PREPARES REGISTRATION LIST
S331
A

FIG. 43

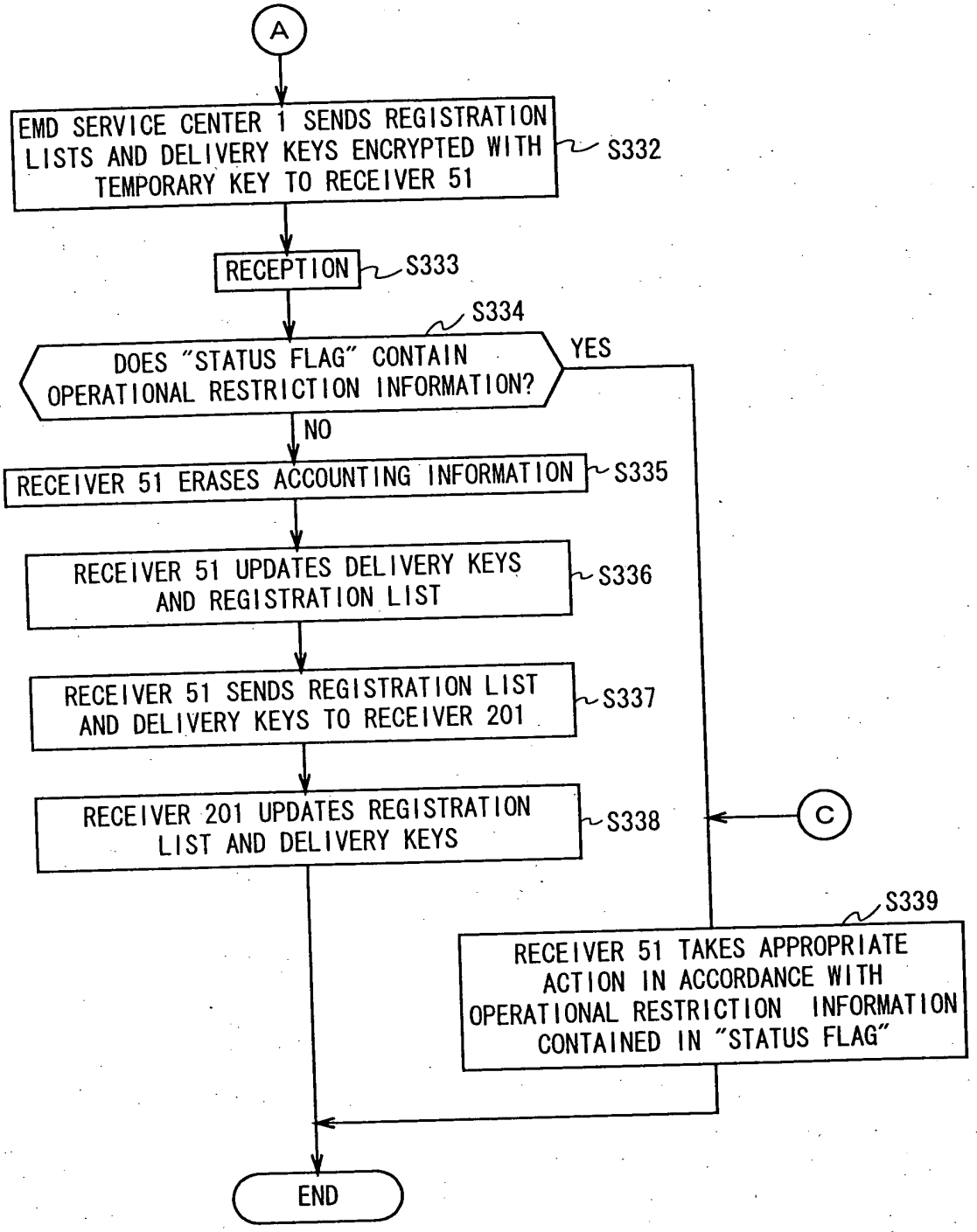

A
EMD SERVICE CENTER 1 SENDS REGISTRATION LISTS AND DELIVERY KEYS ENCRYPTED WITH TEMPORARY KEY TO RECEIVER 51
S332
RECEPTION
S333
S334
DOES "STATUS FLAG" CONTAIN OPERATIONAL RESTRICTION INFORMATION?
YES
NO
RECEIVER 51 ERASES ACCOUNTING INFORMATION
S335
RECEIVER 51 UPDATES DELIVERY KEYS AND REGISTRATION LIST
S336
RECEIVER 51 SENDS REGISTRATION LIST AND DELIVERY KEYS TO RECEIVER 201
S337
RECEIVER 201 UPDATES REGISTRATION LIST AND DELIVERY KEYS
S338
C
S339
RECEIVER 51 TAKES APPROPRIATE ACTION IN ACCORDANCE WITH OPERATIONAL RESTRICTION INFORMATION CONTAINED IN "STATUS FLAG"
END

FIG. 44

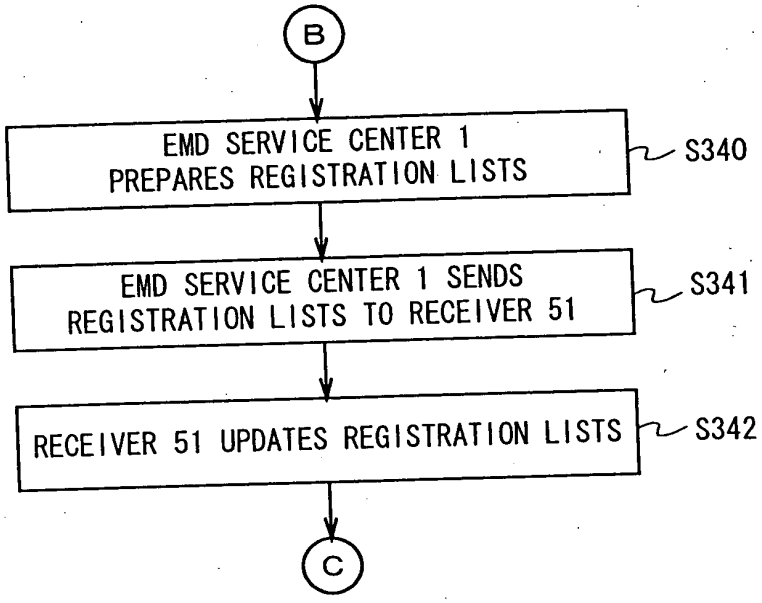

B
EMD SERVICE CENTER 1 PREPARES REGISTRATION LISTS
S340
EMD SERVICE CENTER 1 SENDS REGISTRATION LISTS TO RECEIVER 51
S341
RECEIVER 51 UPDATES REGISTRATION LISTS
S342
C

FIG. 45

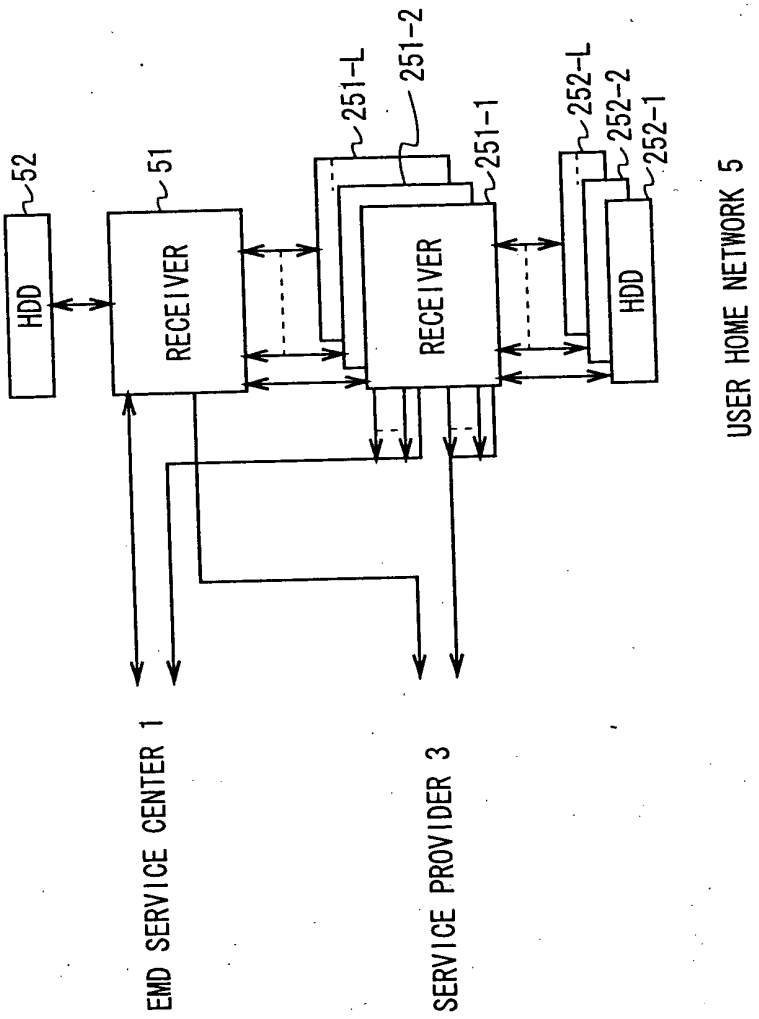

HDD
52
RECEIVER
51
251-L
251-2
251-1
RECEIVER
252-L
252-2
252-1
HDD
USER HOME NETWORK 5
EMD SERVICE CENTER 1
SERVICE PROVIDER 3

FIG. 46

LIST SECTION

SAM ID	USER ID	PURCHASING	ACCOUNTING	EQUIPMENT BILLED	MASTER EQUIPMENT	STATUS FLAG	SIGNATURE TO CONDITIONS	SIGNATURE TO REGISTRATION LIST
ID OF SAM 62	ID OF USER	YES	YES	ID OF SAM 62	NONE	NO RESTRICTION	××××	××××
ID OF SAM	ID OF USER	YES	NO	ID OF SAM 62	NONE	NO RESTRICTION	××××	
ID OF SAM	ID OF USER	YES	NO	ID OF SAM 62	NONE	NO RESTRICTION	××××	
.....	.....	.....	.....	.....	.....	.....	.....	

REGISTRATION CONDITIONS OF RECEIVER 51
REGISTRATION CONDITIONS OF RECEIVER 251-1
REGISTRATION CONDITIONS OF RECEIVER 251-2
.....

SAM INFORMATION SECTION

SAM ID ID OF SAM 62
VALIDITY PERIOD ××××
VERSION NUMBER ××××
NUMBER OF EQUIPMENT CONNECTED L+1

FIG. 47

	SAM ID	USER ID	PURCHA-SING	ACCOU-NTING	EQUIPMENT BILLED	MASTER EQUIPMENT	STATUS FLAG	SIGNATURE TO CONDITIONS	SIGNATURE TO REGISTRATION LIST
REGISTRATION CONDITIONS OF RECEIVER 51	ID OF SAM 62	ID OF USER	YES	YES	ID OF SAM 62	NONE	NO RESTRICTION	××××	××××
REGISTRATION CONDITIONS OF RECEIVER 251-1	ID OF SAM	ID OF USER	YES	NO	ID OF SAM 62	NONE	NO RESTRICTION	××××	
REGISTRATION CONDITIONS OF RECEIVER 251-2	ID OF SAM	ID OF USER	YES	NO	ID OF SAM 62	NONE	NO RESTRICTION	××××	
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	

LIST SECTION

	ID OF SAM OF RECEIVER 251-1
SAM ID	
VALIDITY PERIOD	××××
VERSION NUMBER	××××
NUMBER OF EQUIPMENT CONNECTED	2

SAM INFORMATION SECTION

FIG. 48

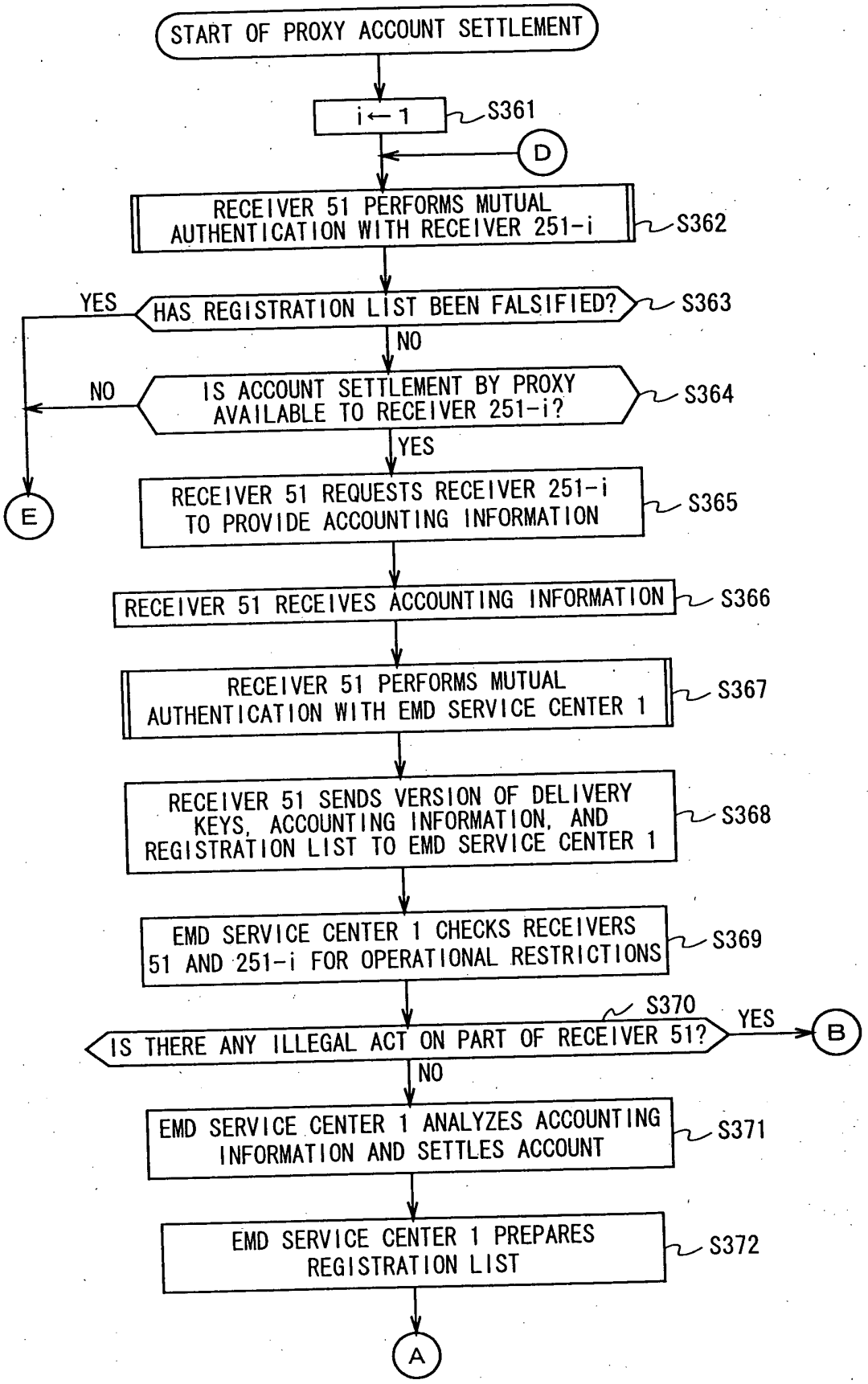

START OF PROXY ACCOUNT SETTLEMENT
i←1
S361
D
RECEIVER 51 PERFORMS MUTUAL AUTHENTICATION WITH RECEIVER 251-i
S362
YES
HAS REGISTRATION LIST BEEN FALSIFIED?
S363
NO
NO
IS ACCOUNT SETTLEMENT BY PROXY AVAILABLE TO RECEIVER 251-i?
S364
YES
E
RECEIVER 51 REQUESTS RECEIVER 251-i TO PROVIDE ACCOUNTING INFORMATION
S365
RECEIVER 51 RECEIVES ACCOUNTING INFORMATION
S366
RECEIVER 51 PERFORMS MUTUAL AUTHENTICATION WITH EMD SERVICE CENTER 1
S367
RECEIVER 51 SENDS VERSION OF DELIVERY KEYS, ACCOUNTING INFORMATION, AND REGISTRATION LIST TO EMD SERVICE CENTER 1
S368
EMD SERVICE CENTER 1 CHECKS RECEIVERS 51 AND 251-i FOR OPERATIONAL RESTRICTIONS
S369
S370
IS THERE ANY ILLEGAL ACT ON PART OF RECEIVER 51?
YES
B
NO
EMD SERVICE CENTER 1 ANALYZES ACCOUNTING INFORMATION AND SETTLES ACCOUNT
S371
EMD SERVICE CENTER 1 PREPARES REGISTRATION LIST
S372
A

FIG. 49

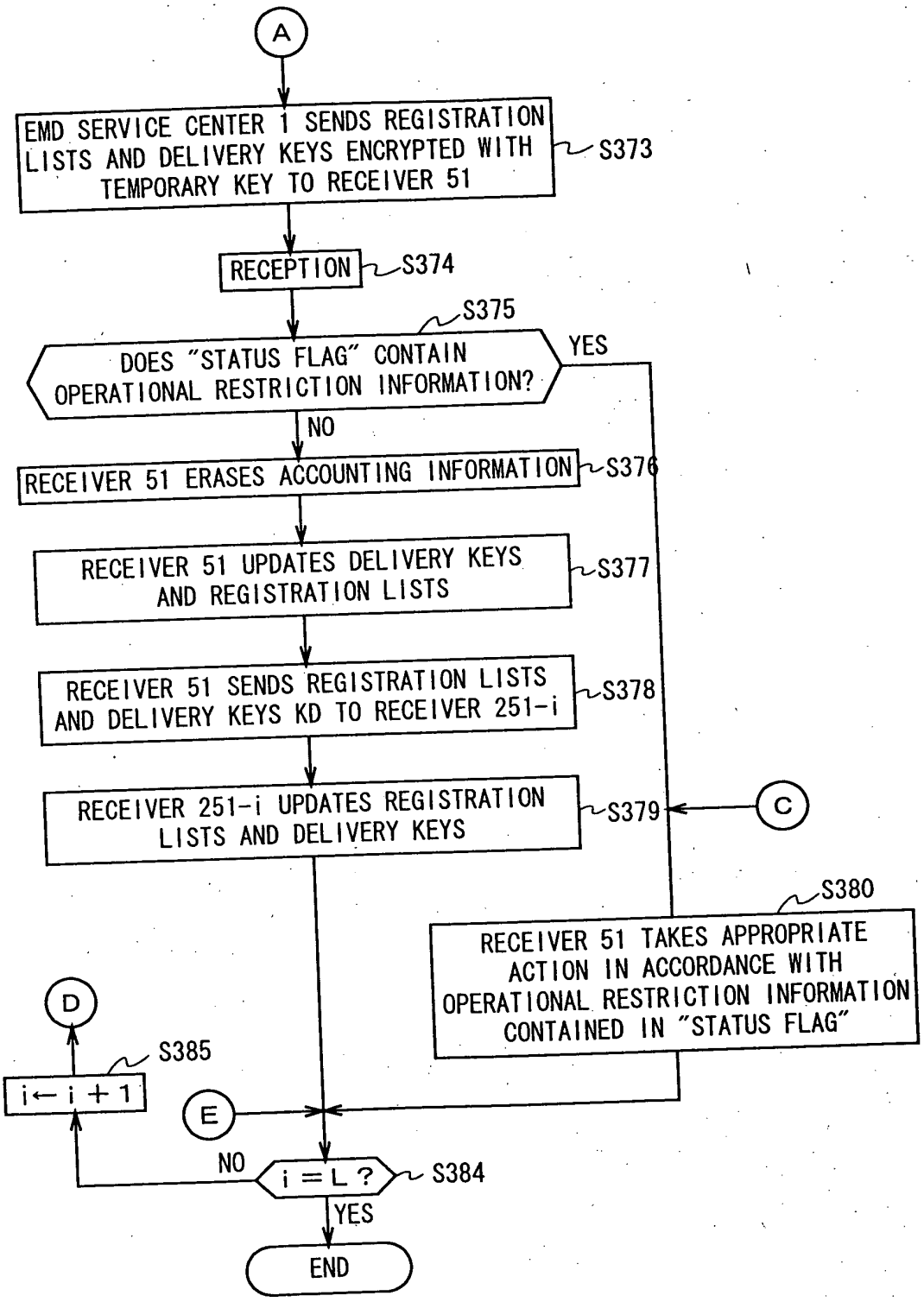

A
EMD SERVICE CENTER 1 SENDS REGISTRATION LISTS AND DELIVERY KEYS ENCRYPTED WITH TEMPORARY KEY TO RECEIVER 51
S373
RECEPTION
S374
S375
DOES "STATUS FLAG" CONTAIN OPERATIONAL RESTRICTION INFORMATION?
YES
NO
RECEIVER 51 ERASES ACCOUNTING INFORMATION
S376
RECEIVER 51 UPDATES DELIVERY KEYS AND REGISTRATION LISTS
S377
RECEIVER 51 SENDS REGISTRATION LISTS AND DELIVERY KEYS KD TO RECEIVER 251-i
S378
RECEIVER 251-i UPDATES REGISTRATION LISTS AND DELIVERY KEYS
S379
C
S380
RECEIVER 51 TAKES APPROPRIATE ACTION IN ACCORDANCE WITH OPERATIONAL RESTRICTION INFORMATION CONTAINED IN "STATUS FLAG"
D
S385
i ← i + 1
E
NO
i = L ?
S384
YES
END

FIG. 50

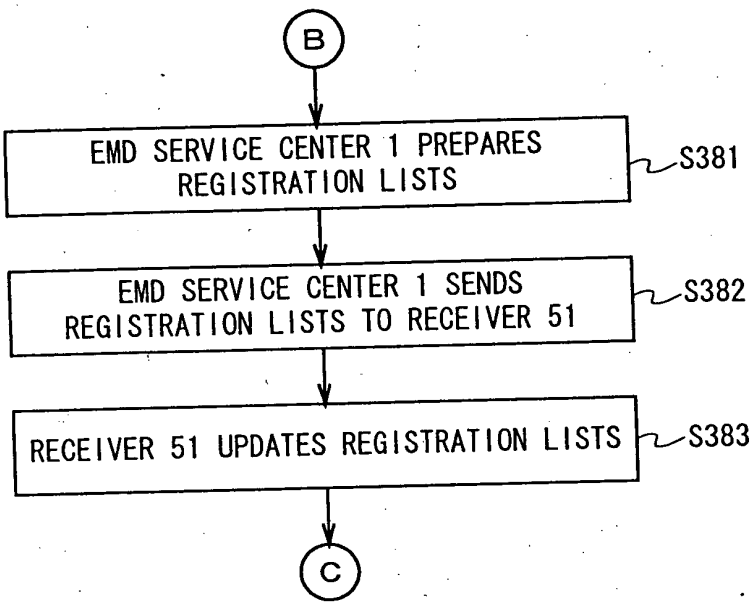

B
EMD SERVICE CENTER 1 PREPARES REGISTRATION LISTS
S381
EMD SERVICE CENTER 1 SENDS REGISTRATION LISTS TO RECEIVER 51
S382
RECEIVER 51 UPDATES REGISTRATION LISTS
S383
C

FIG. 51

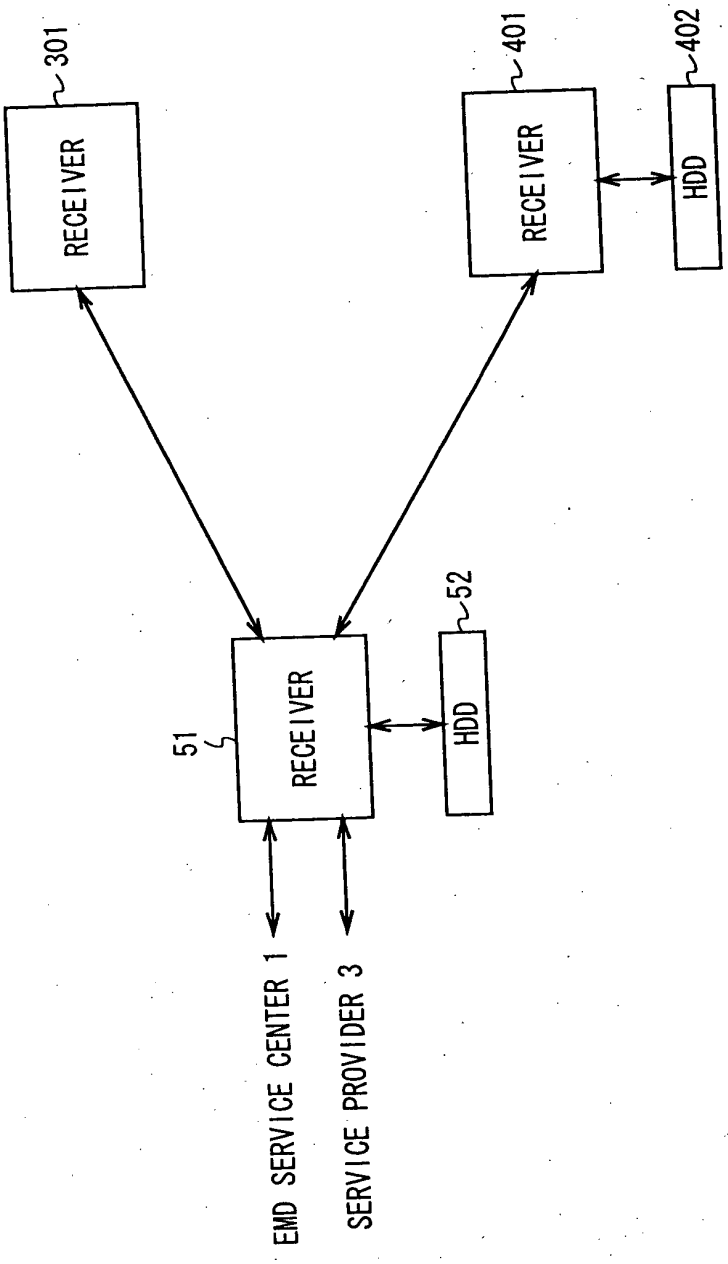

301
RECEIVER
401
RECEIVER
402
HDD
51
RECEIVER
52
HDD
EMD SERVICE CENTER 1
SERVICE PROVIDER 3
USER HOME NETWORK 5

FIG. 52

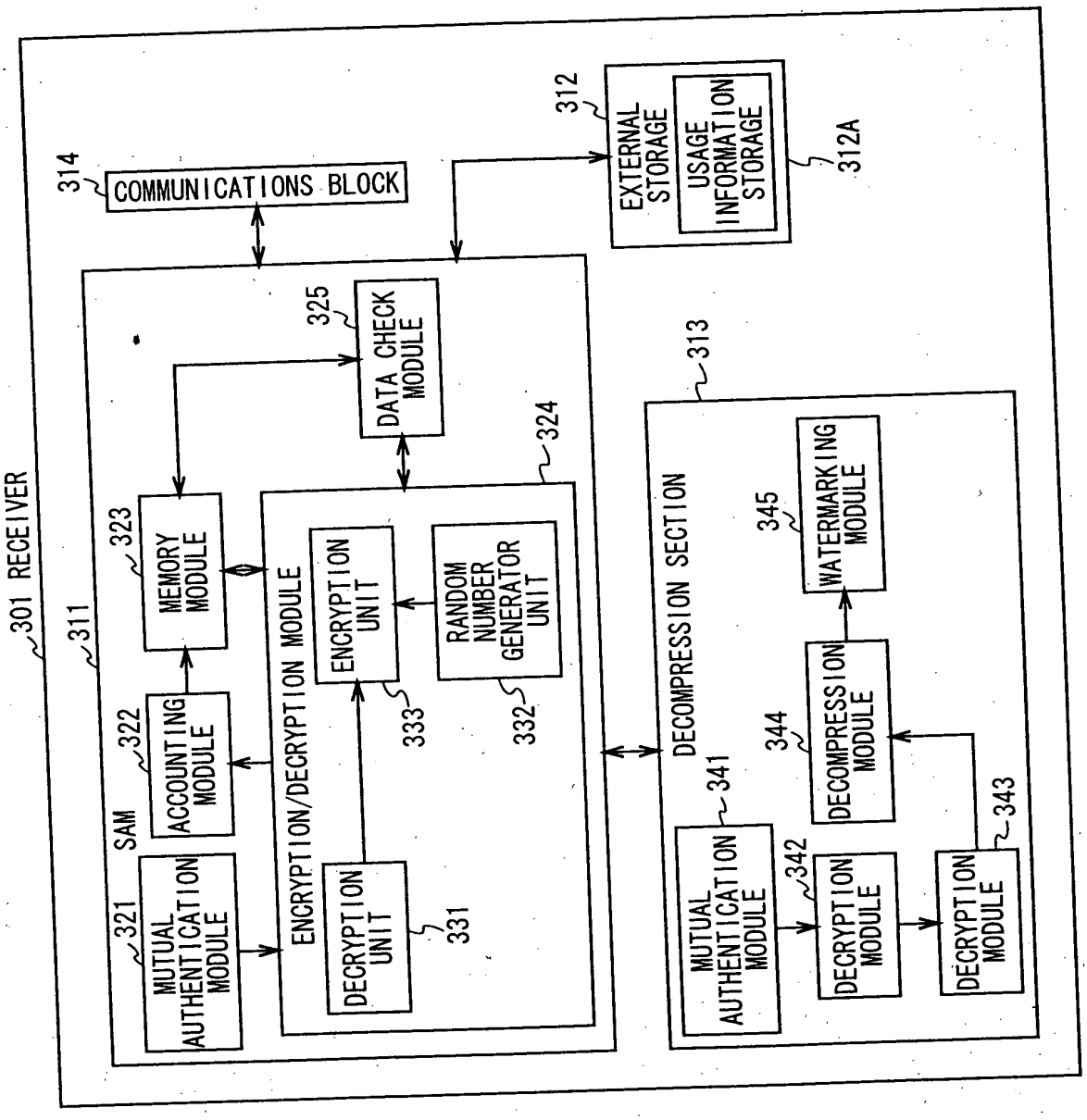

301 RECEIVER
311
SAM
321
MUTUAL AUTHENTICATION MODULE
322
ACCOUNTING MODULE
323
MEMORY MODULE
ENCRYPTION/DECRYPTION MODULE
DECRYPTION UNIT
331
ENCRYPTION UNIT
333
RANDOM NUMBER GENERATOR UNIT
332
324
DATA CHECK MODULE
325
314
COMMUNICATIONS BLOCK
312
EXTERNAL STORAGE
USAGE INFORMATION STORAGE
312A
313
DECOMPRESSION SECTION
341
MUTUAL AUTHENTICATION MODULE
342
DECRYPTION MODULE
343
DECRYPTION MODULE
344
DECOMPRESSION MODULE
345
WATERMARKING MODULE

FIG. 53

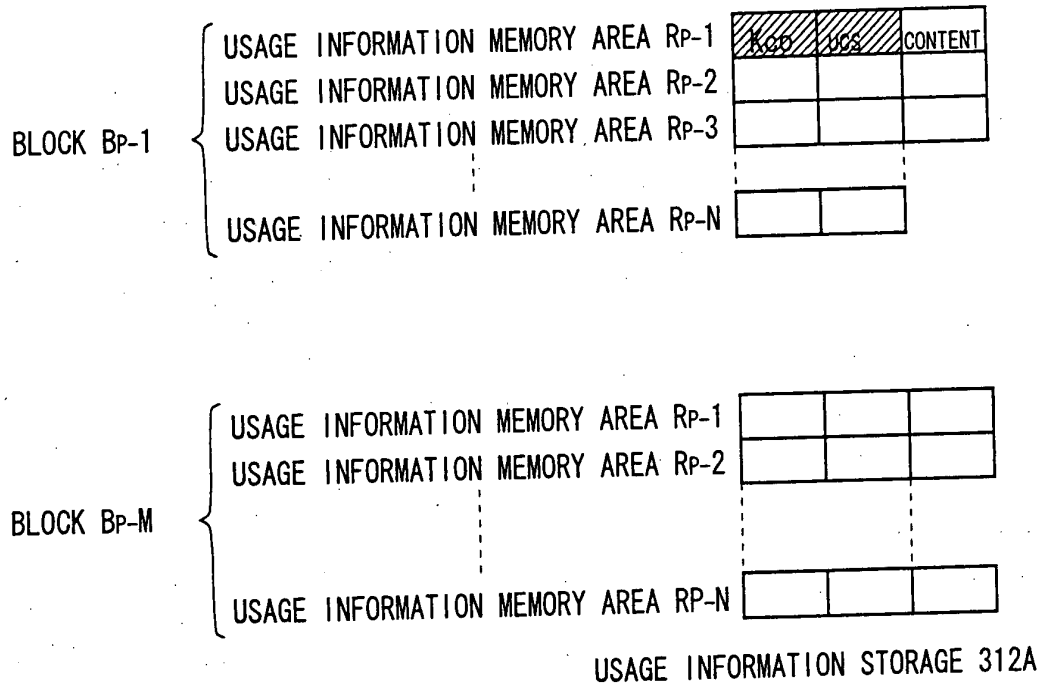

BLOCK BP-1
USAGE INFORMATION MEMORY AREA RP-1
USAGE INFORMATION MEMORY AREA RP-2
USAGE INFORMATION MEMORY AREA RP-3
USAGE INFORMATION MEMORY AREA RP-N
KCD
UCS
CONTENT
BLOCK BP-M
USAGE INFORMATION MEMORY AREA RP-1
USAGE INFORMATION MEMORY AREA RP-2
USAGE INFORMATION MEMORY AREA RP-N
USAGE INFORMATION STORAGE 312A

FIG. 54

REGISTRATION CONDITIONS OF RECEIVER 301

SAM ID	USER ID	PURCHA-SING	ACCOU-NTING	EQUIPMENT BILLED	MASTER EQUIPMENT	STATUS FLAG	SIGNATURE TO CONDITIONS	SIGNATURE TO REGISTRATION LIST
ID OF SAM 311	ID OF USER	NO	NO	NONE	ID OF SAM 62	NO RESTRICTION	××××	××××

LIST SECTION

SAM ID	ID OF SAM 311
VALIDITY PERIOD	××××
VERSION NUMBER	××××
NUMBER OF EQUIPMENT CONNECTED	2

SAM INFORMATION SECTION

REGISTRATION LIST OF RECEIVER 301

FIG. 55

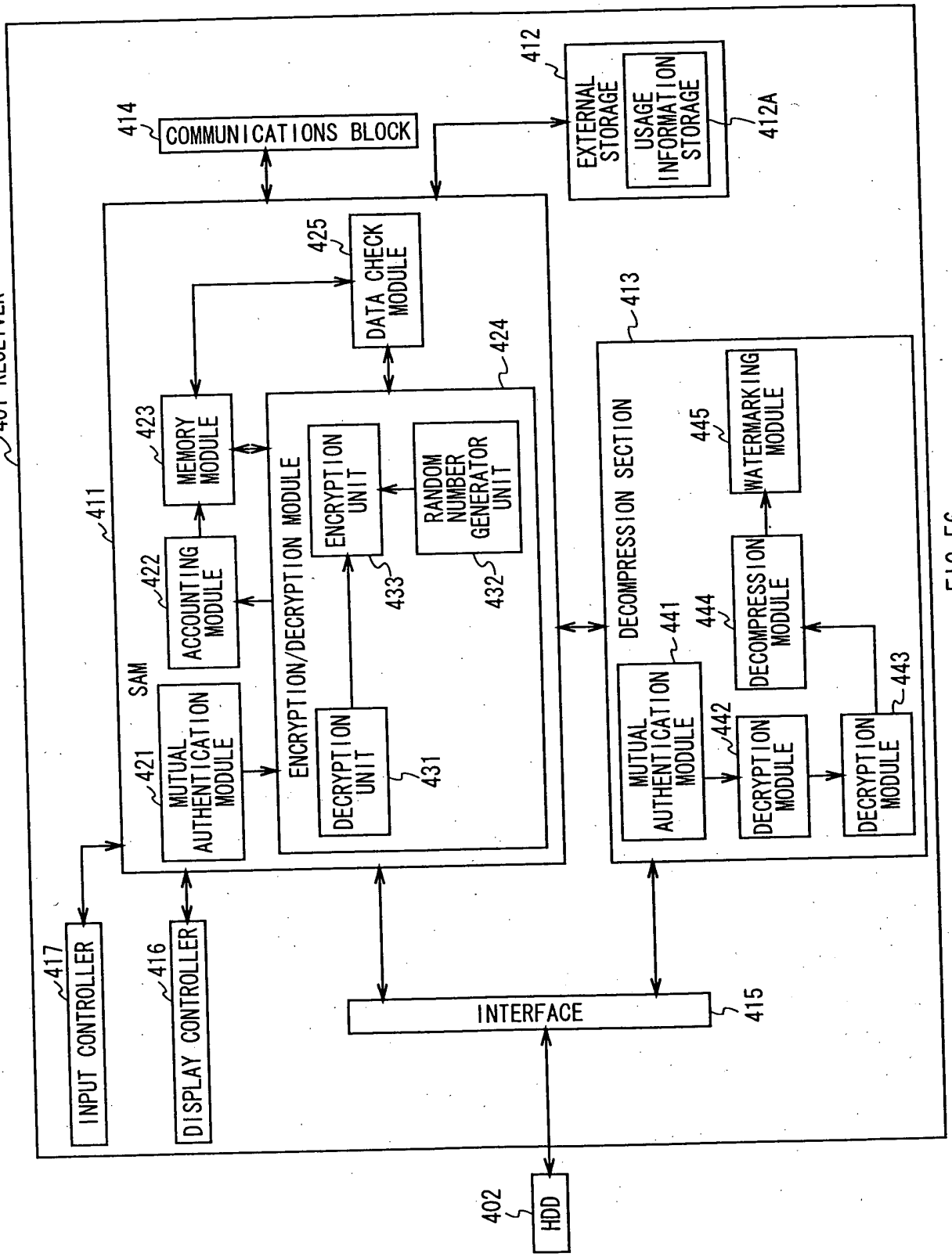

401 RECEIVER
414
COMMUNICATIONS BLOCK
412
EXTERNAL STORAGE
USAGE INFORMATION STORAGE
412A
425
DATA CHECK MODULE
424
413
DECOMPRESSION SECTION
445
WATERMARKING MODULE
423
MEMORY MODULE
411
ENCRYPTION/DECRYPTION MODULE
ENCRYPTION UNIT
RANDOM NUMBER GENERATOR UNIT
433
432
422
ACCOUNTING MODULE
SAM
421
MUTUAL AUTHENTICATION MODULE
DECRYPTION UNIT
431
441
MUTUAL AUTHENTICATION MODULE
444
DECOMPRESSION MODULE
442
DECRYPTION MODULE
443
DECRYPTION MODULE
417
INPUT CONTROLLER
416
DISPLAY CONTROLLER
INTERFACE
415
402
HDD

FIG. 56

REGISTRATION CONDITIONS OF RECEIVER 401

SAM ID	USER ID	PURCHA-SING	ACCOU-NTING	EQUIPMENT BILLED	MASTER EQUIPMENT	STATUS FLAG	SIGNATURE TO CONDITIONS	SIGNATURE TO REGISTRATION LIST
ID OF SAM 411	ID OF USER	NO	NO	NONE	ID OF SAM 62	NO RESTRICTION	××××	××××

LIST SECTION

SAM ID	ID OF SAM 411
VALIDITY PERIOD	××××
VERSION NUMBER	××××
NUMBER OF EQUIPMENT CONNECTED	2

SAM INFORMATION SECTION

REGISTRATION LIST OF RECEIVER 401

FIG. 57

	SAM ID	USER ID	PURCHA-SING	ACCOU-NTING	EQUIPMENT BILLED	MASTER EQUIPMENT	STATUS FLAG	SIGNATURE TO CONDITIONS	SIGNATURE TO REGISTRATION LIST
REGISTRATION CONDITIONS OF RECEIVER 51	ID OF SAM 62	ID OF USER	YES	YES	ID OF SAM 62	NONE	NO RESTRICTION	××××	××××
REGISTRATION CONDITIONS OF RECEIVER 301	ID OF SAM 311	ID OF USER	NO	NO	NONE	ID OF SAM 62	NO RESTRICTION	××××	
REGISTRATION CONDITIONS OF RECEIVER 401	ID OF SAM 411	ID OF USER	NO	NO	NONE	ID OF SAM 62	NO RESTRICTION	××××	

LIST SECTION

REGISTRATION LIST

SAM ID	ID OF SAM 62
VALIDITY PERIOD	××××
VERSION NUMBER	××××
NUMBER OF EQUIPMENT CONNECTED	3

SAM INFORMATION SECTION

FIG. 58

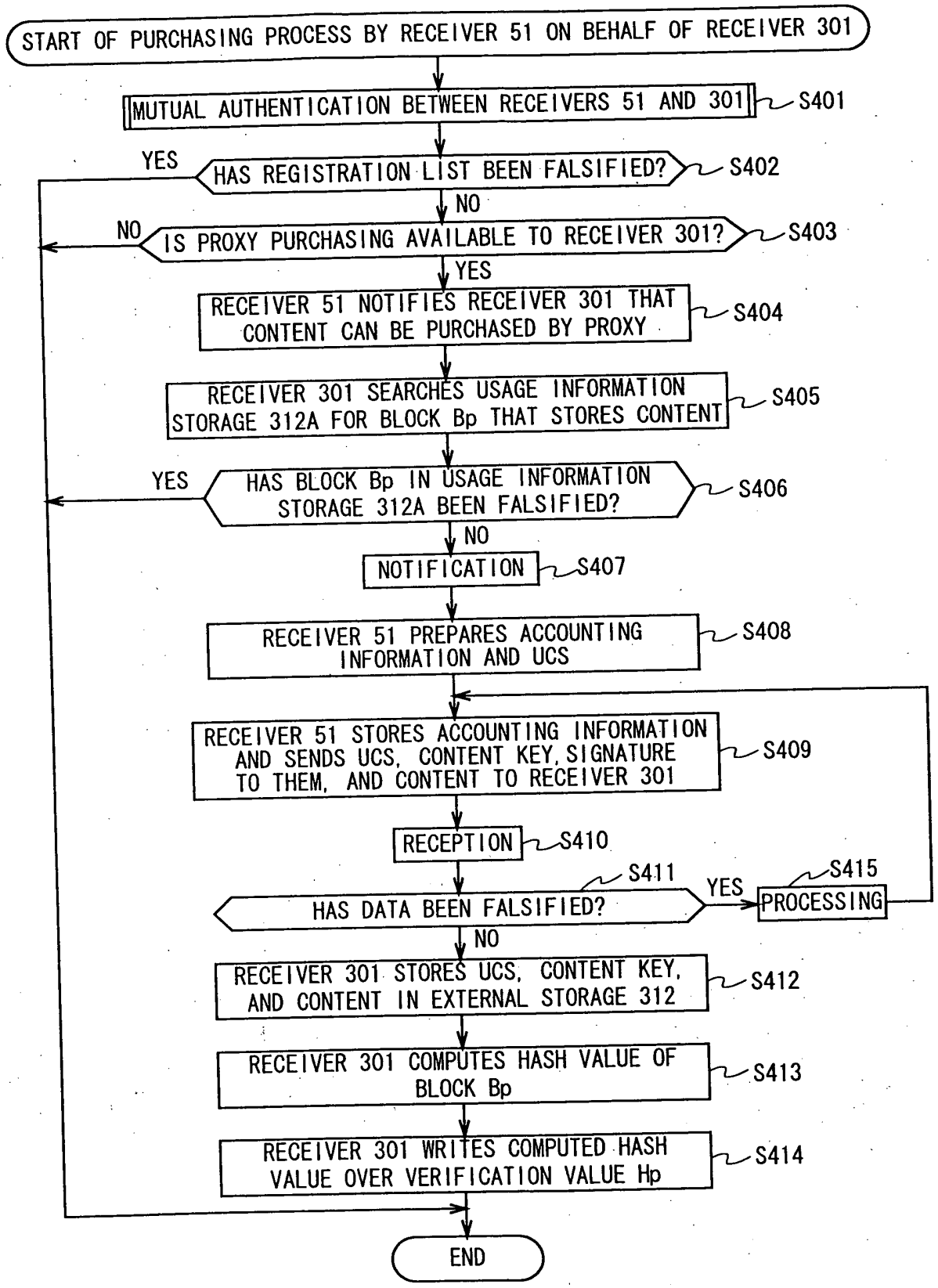

START OF PURCHASING PROCESS BY RECEIVER 51 ON BEHALF OF RECEIVER 301
MUTUAL AUTHENTICATION BETWEEN RECEIVERS 51 AND 301
S401
YES
HAS REGISTRATION LIST BEEN FALSIFIED?
S402
NO
NO
IS PROXY PURCHASING AVAILABLE TO RECEIVER 301?
S403
YES
RECEIVER 51 NOTIFIES RECEIVER 301 THAT CONTENT CAN BE PURCHASED BY PROXY
S404
RECEIVER 301 SEARCHES USAGE INFORMATION STORAGE 312A FOR BLOCK Bp THAT STORES CONTENT
S405
YES
HAS BLOCK Bp IN USAGE INFORMATION STORAGE 312A BEEN FALSIFIED?
S406
NO
NOTIFICATION
S407
RECEIVER 51 PREPARES ACCOUNTING INFORMATION AND UCS
S408
RECEIVER 51 STORES ACCOUNTING INFORMATION AND SENDS UCS, CONTENT KEY, SIGNATURE TO THEM, AND CONTENT TO RECEIVER 301
S409
RECEPTION
S410
S411
YES
S415
HAS DATA BEEN FALSIFIED?
PROCESSING
NO
RECEIVER 301 STORES UCS, CONTENT KEY, AND CONTENT IN EXTERNAL STORAGE 312
S412
RECEIVER 301 COMPUTES HASH VALUE OF BLOCK Bp
S413
RECEIVER 301 WRITES COMPUTED HASH VALUE OVER VERIFICATION VALUE Hp
S414
END

FIG. 59

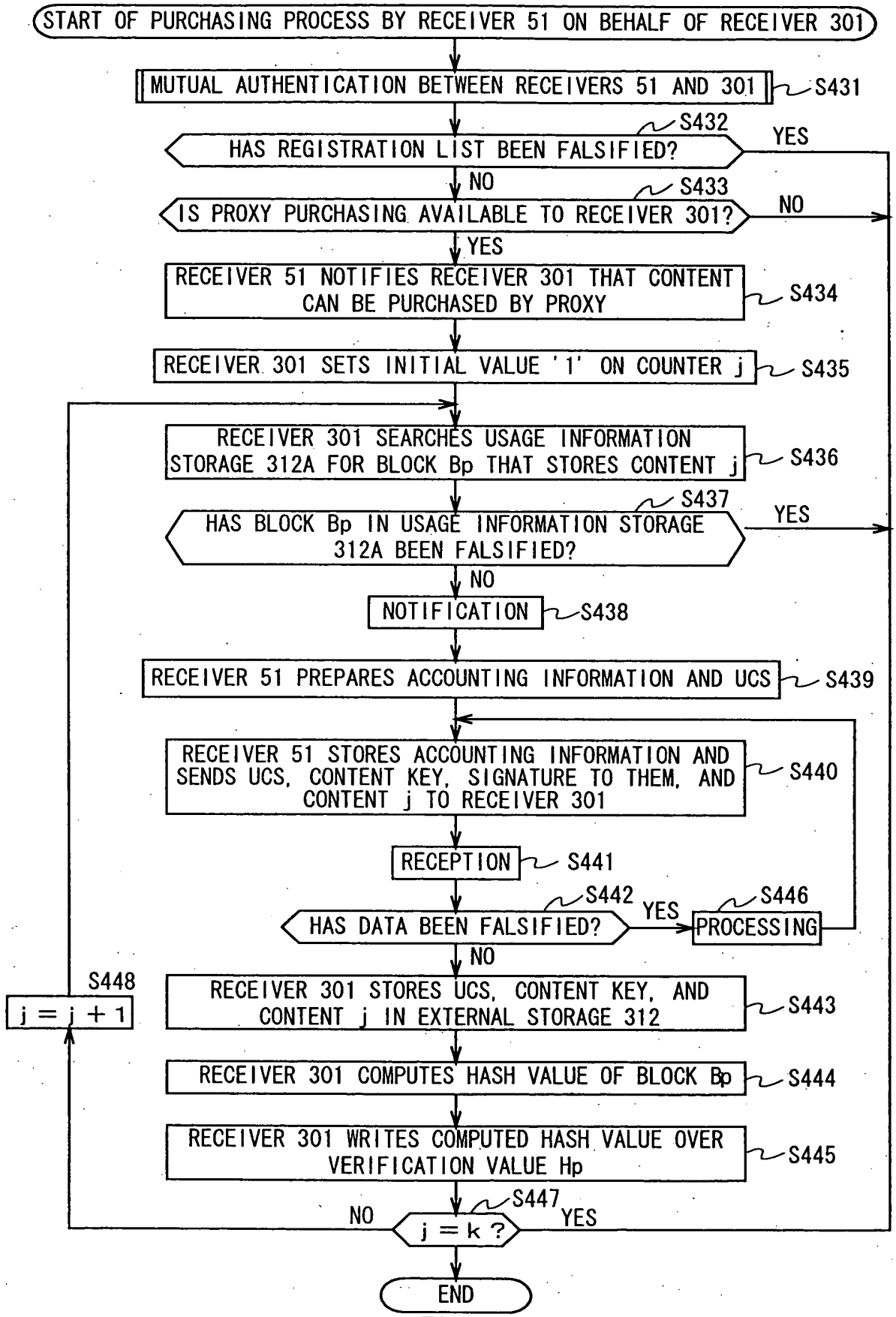

START OF PURCHASING PROCESS BY RECEIVER 51 ON BEHALF OF RECEIVER 301
MUTUAL AUTHENTICATION BETWEEN RECEIVERS 51 AND 301
S431
S432
HAS REGISTRATION LIST BEEN FALSIFIED?
YES
NO
S433
IS PROXY PURCHASING AVAILABLE TO RECEIVER 301?
NO
YES
RECEIVER 51 NOTIFIES RECEIVER 301 THAT CONTENT CAN BE PURCHASED BY PROXY
S434
RECEIVER 301 SETS INITIAL VALUE '1' ON COUNTER j
S435
RECEIVER 301 SEARCHES USAGE INFORMATION STORAGE 312A FOR BLOCK Bp THAT STORES CONTENT j
S436
S437
HAS BLOCK Bp IN USAGE INFORMATION STORAGE 312A BEEN FALSIFIED?
YES
NO
NOTIFICATION
S438
RECEIVER 51 PREPARES ACCOUNTING INFORMATION AND UCS
S439
RECEIVER 51 STORES ACCOUNTING INFORMATION AND SENDS UCS, CONTENT KEY, SIGNATURE TO THEM, AND CONTENT j TO RECEIVER 301
S440
RECEPTION
S441
S442
HAS DATA BEEN FALSIFIED?
YES
S446
PROCESSING
NO
S448
j = j + 1
RECEIVER 301 STORES UCS, CONTENT KEY, AND CONTENT j IN EXTERNAL STORAGE 312
S443
RECEIVER 301 COMPUTES HASH VALUE OF BLOCK Bp
S444
RECEIVER 301 WRITES COMPUTED HASH VALUE OVER VERIFICATION VALUE Hp
S445
S447
NO
j = k ?
YES
END

FIG. 60

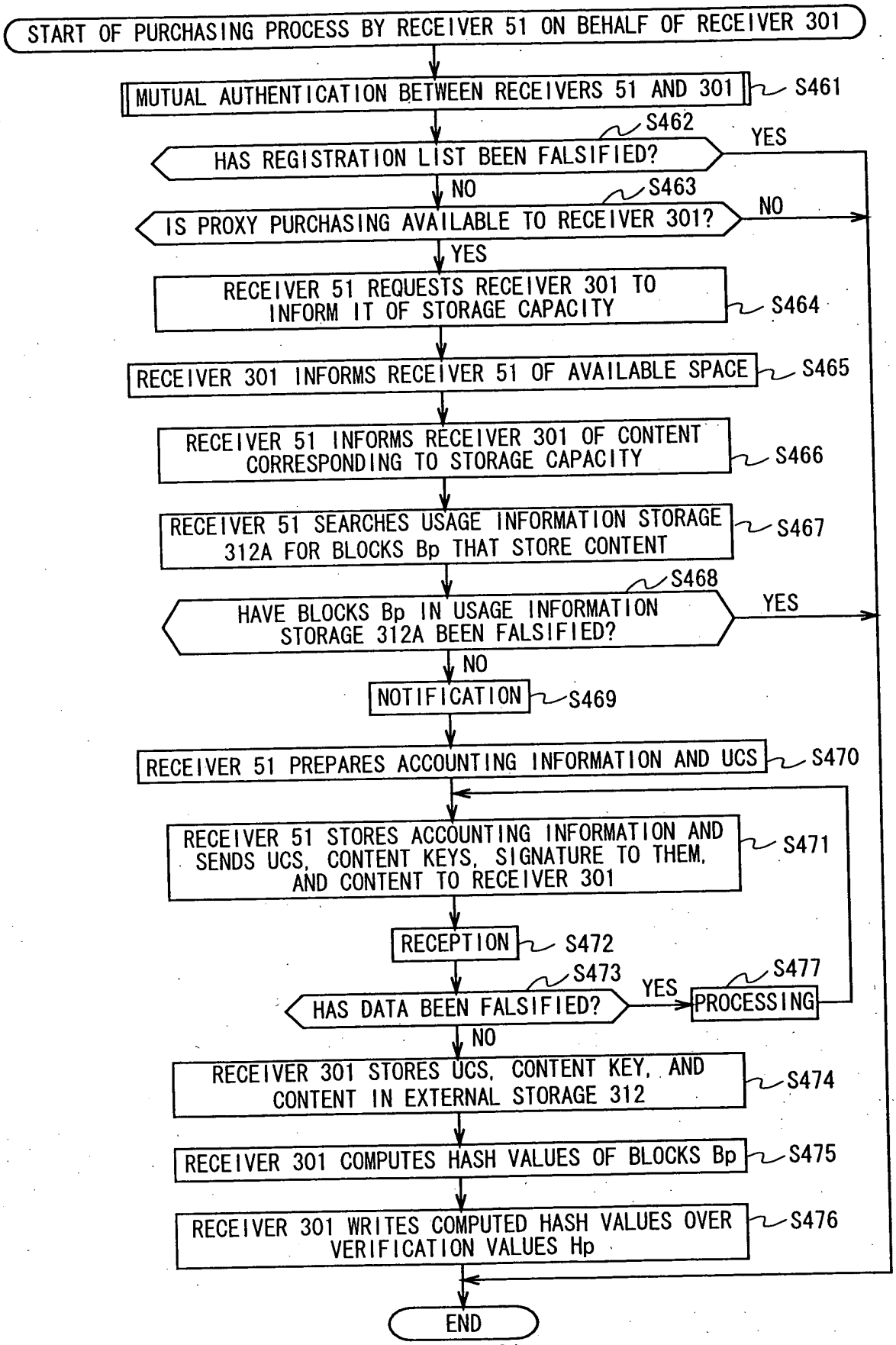

START OF PURCHASING PROCESS BY RECEIVER 51 ON BEHALF OF RECEIVER 301
MUTUAL AUTHENTICATION BETWEEN RECEIVERS 51 AND 301
S461
S462
HAS REGISTRATION LIST BEEN FALSIFIED?
YES
NO
S463
IS PROXY PURCHASING AVAILABLE TO RECEIVER 301?
NO
YES
RECEIVER 51 REQUESTS RECEIVER 301 TO INFORM IT OF STORAGE CAPACITY
S464
RECEIVER 301 INFORMS RECEIVER 51 OF AVAILABLE SPACE
S465
RECEIVER 51 INFORMS RECEIVER 301 OF CONTENT CORRESPONDING TO STORAGE CAPACITY
S466
RECEIVER 51 SEARCHES USAGE INFORMATION STORAGE 312A FOR BLOCKS Bp THAT STORE CONTENT
S467
S468
HAVE BLOCKS Bp IN USAGE INFORMATION STORAGE 312A BEEN FALSIFIED?
YES
NO
NOTIFICATION
S469
RECEIVER 51 PREPARES ACCOUNTING INFORMATION AND UCS
S470
RECEIVER 51 STORES ACCOUNTING INFORMATION AND SENDS UCS, CONTENT KEYS, SIGNATURE TO THEM, AND CONTENT TO RECEIVER 301
S471
RECEPTION
S472
S473
HAS DATA BEEN FALSIFIED?
YES
S477
PROCESSING
NO
RECEIVER 301 STORES UCS, CONTENT KEY, AND CONTENT IN EXTERNAL STORAGE 312
S474
RECEIVER 301 COMPUTES HASH VALUES OF BLOCKS Bp
S475
RECEIVER 301 WRITES COMPUTED HASH VALUES OVER VERIFICATION VALUES Hp
S476
END

FIG. 61

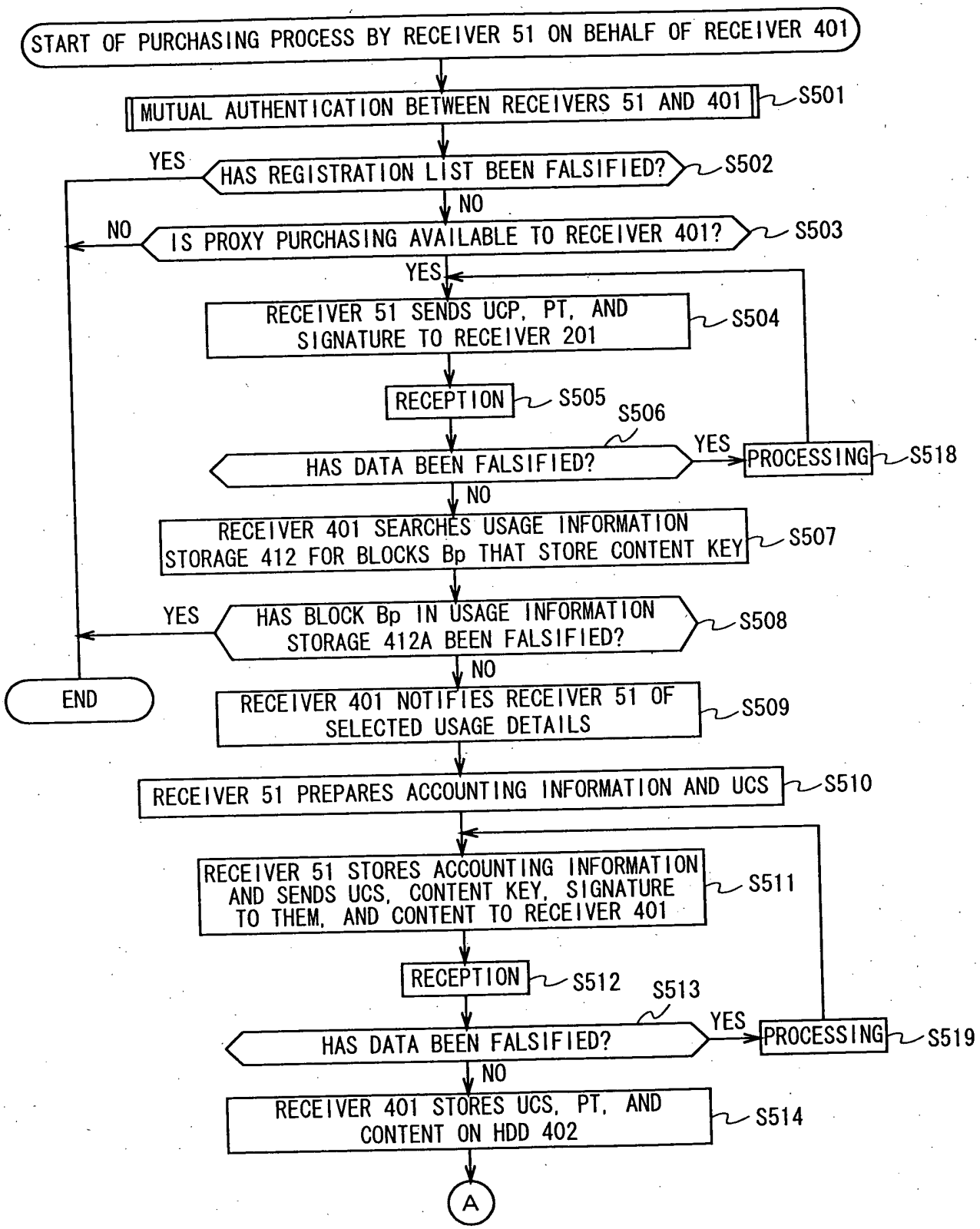

START OF PURCHASING PROCESS BY RECEIVER 51 ON BEHALF OF RECEIVER 401
MUTUAL AUTHENTICATION BETWEEN RECEIVERS 51 AND 401
S501
HAS REGISTRATION LIST BEEN FALSIFIED?
S502
YES
NO
IS PROXY PURCHASING AVAILABLE TO RECEIVER 401?
S503
NO
YES
RECEIVER 51 SENDS UCP, PT, AND SIGNATURE TO RECEIVER 201
S504
RECEPTION
S505
S506
HAS DATA BEEN FALSIFIED?
YES
PROCESSING
S518
NO
RECEIVER 401 SEARCHES USAGE INFORMATION STORAGE 412 FOR BLOCKS Bp THAT STORE CONTENT KEY
S507
HAS BLOCK Bp IN USAGE INFORMATION STORAGE 412A BEEN FALSIFIED?
S508
YES
NO
END
RECEIVER 401 NOTIFIES RECEIVER 51 OF SELECTED USAGE DETAILS
S509
RECEIVER 51 PREPARES ACCOUNTING INFORMATION AND UCS
S510
RECEIVER 51 STORES ACCOUNTING INFORMATION AND SENDS UCS, CONTENT KEY, SIGNATURE TO THEM, AND CONTENT TO RECEIVER 401
S511
RECEPTION
S512
S513
HAS DATA BEEN FALSIFIED?
YES
PROCESSING
S519
NO
RECEIVER 401 STORES UCS, PT, AND CONTENT ON HDD 402
S514
A

FIG. 62

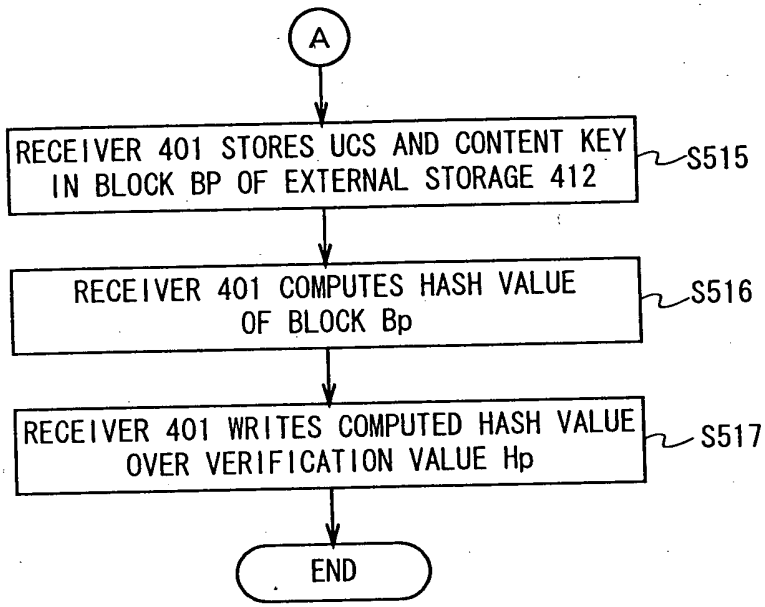

A
RECEIVER 401 STORES UCS AND CONTENT KEY IN BLOCK BP OF EXTERNAL STORAGE 412
S515
RECEIVER 401 COMPUTES HASH VALUE OF BLOCK Bp
S516
RECEIVER 401 WRITES COMPUTED HASH VALUE OVER VERIFICATION VALUE Hp
S517
END

FIG. 63

Explanation of Reference Numerals

1 ... EMD service center, 2 ... content provider, 3 ... service provider, 5 ... user home network, 11 ... service provider management section, 12 ... content provider management section, 13 ...copyright management section, 14 ... key server, 15 ... log data management section, 16 ... profit-sharing section, 17 ... mutual authentication section, 18 ... user management section, 19 ... billing section, 20 ... cashier section, 21 ... audit section, 31 ... content server, 32 ...watermarking section, 33 ... compression section, 34 ... encryption section, 35 ... random number generator section, 36 ... encryption section, 37 ... policy storage section, 38 ... secure container preparation section, 39 ... mutual authentication section, 41 ... content server, 42 ... pricing section, 43 ... policy storage section, 44 ... secure container preparation section, 45 ... mutual authentication section, 51 ... receiver, 52 ... HDD, 61 ...communication block, 62 ... SAM, 63 ... external storage, 64 ... decompression section, 65 ... communication block, 66 ... interface, 67 ... display controller, 68 ... input controller, 71 ... mutual authentication module, 72 ... accounting module, 73 ... memory module, 74 ... encryption/decryption module, 75 ... data check module, 91 ... decryption unit, 92 ... random number generator unit, 93 ... encryption unit, 101 ... mutual authentication module, 102 ... decryption module, 103 ... decryption module, 104 ... decompression module, 105 ... watermarking module, 201 ... receiver, 202 ... HDD,

211 ... communication block, 212 ... SAM, 213 ... external storage, 214 ... decompression section, 215 ... communication block, 216 ... interface, 217 ... display controller, 218 ... input controller, 221 ... mutual authentication module, 222 ... accounting module, 223 ... memory module, 224 ... encryption/decryption module, 225 ... data check module, 231 ... decryption unit, 232 ... random number generator unit, 233 ... encryption unit, 241 ... mutual authentication module, 242 ... decryption module, 243 ... decryption module, 244 ... decompression module, 245 ... watermarking module, 301 ... receiver, 311 ... SAM, 312 ... external storage, 313 ... decompression section, 314 ... communication block, 321 ... mutual authentication module, 322 ... accounting module, 323 ... memory module, 324 ... encryption/decryption module, 325 ... data check module, 331 ... decryption unit, 332 ... random number generator unit, 333 ... encryption unit, 341 ... mutual authentication module, 342 ... decryption module, 344 ... decompression module, 345 ... watermarking module, 401 ... receiver, 402 ... HDD, 411 ... SAM, 412 ... external storage, 413 ... decompression section, 414 ... communication block, 415 ... interface, 416 ... display controller, 417 ... input controller, 421 ... mutual authentication module, 422 ... accounting module, 423 ... memory module, 424 ... encryption/decryption module, 425 ... data check module, 431 ... decryption unit, 432 ... random number generator unit, 433 ... encryption unit, 441 ... mutual authentication module, 442 ... decryption module, 443 ... decryption module, 444 ... decompression module, 445 ... watermarking module.